Service Authorization Reference

Service Authorization Reference

Service Authorization Reference: Service Authorization Reference

Table of Contents

Reference

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

Contents

Actions, resources, and condition keys for AWS services

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

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

The actions table

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

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

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

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

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

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

The resource types table

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

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

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

The condition keys table

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

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

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

Topics

- Actions, resources, and condition keys for Amazon API Gateway Management
- Actions, resources, and condition keys for Amazon API Gateway Management V2
- Actions, resources, and condition keys for AWS App Mesh
- Actions, resources, and condition keys for AWS App Mesh Preview
- Actions, resources, and condition keys for AWS App Runner
- Actions, resources, and condition keys for AWS App Studio
- Actions, resources, and condition keys for AWS App2Container
- Actions, resources, and condition keys for AWS AppConfig
- Actions, resources, and condition keys for AWS AppFabric
- Actions, resources, and condition keys for Amazon AppFlow
- Actions, resources, and condition keys for Amazon AppIntegrations
- Actions, resources, and condition keys for AWS Application Auto Scaling
- Actions, resources, and condition keys for Application Discovery Arsenal
- Actions, resources, and condition keys for AWS Application Discovery Service
- Actions, resources, and condition keys for AWS Application Migration Service
- Actions, resources, and condition keys for Amazon Application Recovery Controller - Zonal Shift
- Actions, resources, and condition keys for AWS Application Transformation Service
- Actions, resources, and condition keys for Amazon AppStream 2.0
- Actions, resources, and condition keys for AWS AppSync
- Actions, resources, and condition keys for Amazon ARC Region switch
- Actions, resources, and condition keys for AWS Artifact
- Actions, resources, and condition keys for Amazon Athena
- Actions, resources, and condition keys for AWS Audit Manager
- Actions, resources, and condition keys for Amazon Aurora DSQL
- Actions, resources, and condition keys for AWS Auto Scaling
- Actions, resources, and condition keys for AWS B2B Data Interchange
- Actions, resources, and condition keys for AWS Backup
- Actions, resources, and condition keys for AWS Backup Gateway
- Actions, resources, and condition keys for AWS Backup Search

- Actions, resources, and condition keys for AWS Backup storage
- Actions, resources, and condition keys for AWS Batch
- Actions, resources, and condition keys for Amazon Bedrock
- Actions, resources, and condition keys for Amazon Bedrock Agentcore
- Actions, resources, and condition keys for Amazon Bedrock Powered by AWS Mantle
- Actions, resources, and condition keys for AWS Billing
- Actions, resources, and condition keys for AWS Billing and Cost Management Dashboards
- Actions, resources, and condition keys for AWS Billing And Cost Management Data Exports
- Actions, resources, and condition keys for AWS Billing And Cost Management Pricing Calculator
- Actions, resources, and condition keys for AWS Billing And Cost Management Recommended Actions
- Actions, resources, and condition keys for AWS Billing Conductor
- Actions, resources, and condition keys for AWS Billing Console
- Actions, resources, and condition keys for Amazon Braket
- Actions, resources, and condition keys for AWS Budget Service
- Actions, resources, and condition keys for AWS BugBust
- Actions, resources, and condition keys for AWS Certificate Manager
- Actions, resources, and condition keys for AWS Chatbot
- Actions, resources, and condition keys for Amazon Chime
- Actions, resources, and condition keys for AWS Clean Rooms
- Actions, resources, and condition keys for AWS Clean Rooms ML
- Actions, resources, and condition keys for AWS Cloud Control API
- Actions, resources, and condition keys for Amazon Cloud Directory
- Actions, resources, and condition keys for AWS Cloud Map
- Actions, resources, and condition keys for AWS Cloud9
- Actions, resources, and condition keys for AWS CloudFormation
- Actions, resources, and condition keys for Amazon CloudFront
- Actions, resources, and condition keys for Amazon CloudFront KeyValueStore
- Actions, resources, and condition keys for AWS CloudHSM
- Actions, resources, and condition keys for Amazon CloudSearch

- Actions, resources, and condition keys for AWS CloudShell
- Actions, resources, and condition keys for AWS CloudTrail
- Actions, resources, and condition keys for AWS CloudTrail Data
- 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 Application Signals
- Actions, resources, and condition keys for Amazon CloudWatch Evidently
- Actions, resources, and condition keys for Amazon CloudWatch Internet Monitor
- Actions, resources, and condition keys for Amazon CloudWatch Logs
- Actions, resources, and condition keys for Amazon CloudWatch Network Synthetic Monitor
- Actions, resources, and condition keys for Amazon CloudWatch Observability Access Manager
- Actions, resources, and condition keys for Amazon CloudWatch Observability Admin Service
- Actions, resources, and condition keys for AWS CloudWatch RUM
- Actions, resources, and condition keys for Amazon CloudWatch Synthetics
- Actions, resources, and condition keys for AWS CodeArtifact
- Actions, resources, and condition keys for AWS CodeBuild
- Actions, resources, and condition keys for Amazon CodeCatalyst
- Actions, resources, and condition keys for AWS CodeCommit
- Actions, resources, and condition keys for AWS CodeConnections
- Actions, resources, and condition keys for AWS CodeDeploy
- Actions, resources, and condition keys for AWS CodeDeploy secure host commands service
- Actions, resources, and condition keys for Amazon CodeGuru
- Actions, resources, and condition keys for Amazon CodeGuru Profiler
- Actions, resources, and condition keys for Amazon CodeGuru Reviewer
- Actions, resources, and condition keys for Amazon CodeGuru Security
- Actions, resources, and condition keys for AWS CodePipeline
- Actions, resources, and condition keys for AWS CodeStar
- Actions, resources, and condition keys for AWS CodeStar Connections
- Actions, resources, and condition keys for AWS CodeStar Notifications

- Actions, resources, and condition keys for Amazon CodeWhisperer
- Actions, resources, and condition keys for Amazon Cognito Identity
- Actions, resources, and condition keys for Amazon Cognito Sync
- Actions, resources, and condition keys for Amazon Cognito User Pools
- Actions, resources, and condition keys for Amazon Comprehend
- Actions, resources, and condition keys for Amazon Comprehend Medical
- Actions, resources, and condition keys for AWS Compute Optimizer
- Actions, resources, and condition keys for AWS Compute Optimizer Automation
- Actions, resources, and condition keys for AWS Config
- Actions, resources, and condition keys for Amazon Connect
- Actions, resources, and condition keys for Amazon Connect Cases
- Actions, resources, and condition keys for Amazon Connect Customer Profiles
- Actions, resources, and condition keys for Amazon Connect Health
- Actions, resources, and condition keys for Amazon Connect Outbound Campaigns
- Actions, resources, and condition keys for Amazon Connect Voice ID
- Actions, resources, and condition keys for AWS Connector Service
- Actions, resources, and condition keys for AWS Management Console Mobile App
- Actions, resources, and condition keys for AWS Consolidated Billing
- Actions, resources, and condition keys for AWS Control Catalog
- Actions, resources, and condition keys for AWS Control Tower
- Actions, resources, and condition keys for AWS Cost and Usage Report
- Actions, resources, and condition keys for AWS Cost Explorer Service
- Actions, resources, and condition keys for AWS Cost Optimization Hub
- Actions, resources, and condition keys for AWS Customer Verification Service
- Actions, resources, and condition keys for AWS Data Exchange
- Actions, resources, and condition keys for Amazon Data Lifecycle Manager
- Actions, resources, and condition keys for AWS Data Pipeline
- Actions, resources, and condition keys for AWS Database Migration Service
- Actions, resources, and condition keys for Database Query Metadata Service

- Actions, resources, and condition keys for AWS DataSync
- Actions, resources, and condition keys for Amazon DataZone
- Actions, resources, and condition keys for AWS Deadline Cloud
- Actions, resources, and condition keys for Amazon Detective
- Actions, resources, and condition keys for AWS Device Farm
- Actions, resources, and condition keys for AWS DevOps Agent Service
- Actions, resources, and condition keys for Amazon DevOps Guru
- Actions, resources, and condition keys for AWS Diagnostic tools
- Actions, resources, and condition keys for AWS Direct Connect
- Actions, resources, and condition keys for AWS Directory Service
- Actions, resources, and condition keys for AWS Directory Service Data
- Actions, resources, and condition keys for Amazon DocumentDB Elastic Clusters
- 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 ECS MCP Service
- Actions, resources, and condition keys for Amazon EKS Auth
- Actions, resources, and condition keys for Amazon EKS MCP Server
- Actions, resources, and condition keys for AWS 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 Registry Public
- Actions, resources, and condition keys for Amazon Elastic Container Service
- Actions, resources, and condition keys for AWS Elastic Disaster Recovery
- Actions, resources, and condition keys for Amazon Elastic File System
- Actions, resources, and condition keys for Amazon Elastic Kubernetes Service

- Actions, resources, and condition keys for AWS Elastic Load Balancing
- Actions, resources, and condition keys for AWS Elastic Load Balancing V2
- Actions, resources, and condition keys for Amazon Elastic MapReduce
- Actions, resources, and condition keys for Amazon Elastic Transcoder
- Actions, resources, and condition keys for Amazon Elastic VMware Service
- Actions, resources, and condition keys for Amazon ElastiCache
- Actions, resources, and condition keys for AWS Elemental Appliances and Software
- Actions, resources, and condition keys for AWS Elemental Appliances and Software Activation Service
- Actions, resources, and condition keys for AWS Elemental Inference
- Actions, resources, and condition keys for AWS Elemental MediaConnect
- Actions, resources, and condition keys for AWS Elemental MediaConvert
- Actions, resources, and condition keys for AWS Elemental MediaLive
- Actions, resources, and condition keys for AWS Elemental MediaPackage
- Actions, resources, and condition keys for AWS Elemental MediaPackage V2
- Actions, resources, and condition keys for AWS Elemental MediaPackage VOD
- Actions, resources, and condition keys for AWS Elemental MediaStore
- Actions, resources, and condition keys for AWS Elemental MediaTailor
- Actions, resources, and condition keys for AWS Elemental Support Cases
- Actions, resources, and condition keys for AWS Elemental Support Content
- Actions, resources, and condition keys for Amazon EMR on EKS (EMR Containers)
- Actions, resources, and condition keys for Amazon EMR Serverless
- Actions, resources, and condition keys for AWS End User Messaging SMS and Voice V2
- Actions, resources, and condition keys for AWS End User Messaging Social
- Actions, resources, and condition keys for AWS Entity Resolution
- Actions, resources, and condition keys for Amazon EventBridge
- Actions, resources, and condition keys for Amazon EventBridge Pipes
- Actions, resources, and condition keys for Amazon EventBridge Scheduler
- Actions, resources, and condition keys for Amazon EventBridge Schemas
- Actions, resources, and condition keys for AWS Fault Injection Service

- Actions, resources, and condition keys for Amazon FinSpace
- Actions, resources, and condition keys for Amazon FinSpace API
- Actions, resources, and condition keys for AWS Firewall Manager
- Actions, resources, and condition keys for Amazon Forecast
- Actions, resources, and condition keys for Amazon Fraud Detector
- Actions, resources, and condition keys for AWS 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 Servers
- Actions, resources, and condition keys for Amazon GameLift Streams
- Actions, resources, and condition keys for AWS Global Accelerator
- Actions, resources, and condition keys for AWS Glue
- Actions, resources, and condition keys for AWS Glue DataBrew
- Actions, resources, and condition keys for AWS Ground Station
- Actions, resources, and condition keys for Amazon GroundTruth Labeling
- Actions, resources, and condition keys for Amazon GuardDuty
- Actions, resources, and condition keys for AWS Health APIs and Notifications
- Actions, resources, and condition keys for AWS HealthImaging
- Actions, resources, and condition keys for AWS HealthLake
- Actions, resources, and condition keys for AWS HealthOmics
- Actions, resources, and condition keys for Amazon Honeycode
- Actions, resources, and condition keys for AWS IAM Access Analyzer
- Actions, resources, and condition keys for AWS IAM Identity Center
- Actions, resources, and condition keys for AWS IAM Identity Center directory
- Actions, resources, and condition keys for AWS IAM Identity Center OIDC service
- Actions, resources, and condition keys for AWS Identity and Access Management (IAM)
- Actions, resources, and condition keys for AWS Identity and Access Management Roles Anywhere
- Actions, resources, and condition keys for AWS Identity Store
- Actions, resources, and condition keys for AWS Identity Store Auth

- Actions, resources, and condition keys for AWS Identity Sync
- Actions, resources, and condition keys for AWS Import Export Disk Service
- Actions, resources, and condition keys for Amazon Inspector
- Actions, resources, and condition keys for Amazon Inspector2
- Actions, resources, and condition keys for Amazon Inspector2 Telemetry Channel
- Actions, resources, and condition keys for Amazon InspectorScan
- Actions, resources, and condition keys for Amazon Interactive Video Service
- Actions, resources, and condition keys for Amazon Interactive Video Service Chat
- Actions, resources, and condition keys for AWS Interconnect
- Actions, resources, and condition keys for AWS Invoicing Service
- Actions, resources, and condition keys for AWS IoT
- Actions, resources, and condition keys for AWS IoT Analytics
- Actions, resources, and condition keys for AWS IoT Core Device Advisor
- Actions, resources, and condition keys for AWS IoT Device Tester
- Actions, resources, and condition keys for AWS IoT Events
- Actions, resources, and condition keys for AWS IoT Fleet Hub for Device Management
- Actions, resources, and condition keys for AWS IoT FleetWise
- Actions, resources, and condition keys for AWS IoT Greengrass
- Actions, resources, and condition keys for AWS IoT Greengrass V2
- Actions, resources, and condition keys for AWS IoT Jobs DataPlane
- Actions, resources, and condition keys for AWS IoT Managed Integrations
- Actions, resources, and condition keys for AWS IoT SiteWise
- Actions, resources, and condition keys for AWS IoT TwinMaker
- Actions, resources, and condition keys for AWS IoT Wireless
- Actions, resources, and condition keys for AWS IQ
- Actions, resources, and condition keys for AWS IQ Permissions
- Actions, resources, and condition keys for Amazon Kendra
- Actions, resources, and condition keys for Amazon Kendra Intelligent Ranking
- Actions, resources, and condition keys for AWS Key Management Service

- Actions, resources, and condition keys for Amazon Keyspaces (for Apache Cassandra)
- 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 AWS Lake Formation
- Actions, resources, and condition keys for AWS Lambda
- Actions, resources, and condition keys for AWS Launch Wizard
- Actions, resources, and condition keys for Amazon Lex
- Actions, resources, and condition keys for Amazon Lex V2
- Actions, resources, and condition keys for AWS License Manager
- Actions, resources, and condition keys for AWS License Manager Linux Subscriptions Manager
- Actions, resources, and condition keys for AWS License Manager User Subscriptions
- Actions, resources, and condition keys for Amazon Lightsail
- Actions, resources, and condition keys for Amazon Location
- Actions, resources, and condition keys for Amazon Location Service Maps
- Actions, resources, and condition keys for Amazon Location Service Places
- Actions, resources, and condition keys for Amazon Location Service Routes
- Actions, resources, and condition keys for Amazon Lookout for Equipment
- Actions, resources, and condition keys for Amazon Lookout for Metrics
- Actions, resources, and condition keys for Amazon Lookout for Vision
- Actions, resources, and condition keys for Amazon Machine Learning
- Actions, resources, and condition keys for Amazon Macie
- Actions, resources, and condition keys for AWS Mainframe Modernization Application Testing
- Actions, resources, and condition keys for AWS Mainframe Modernization Service
- Actions, resources, and condition keys for Amazon Managed Blockchain
- Actions, resources, and condition keys for Amazon Managed Blockchain Query
- Actions, resources, and condition keys for Amazon Managed Grafana

- Actions, resources, and condition keys for Amazon Managed Service for Prometheus
- Actions, resources, and condition keys for Amazon Managed Streaming for Apache Kafka
- Actions, resources, and condition keys for Amazon Managed Streaming for Kafka Connect
- Actions, resources, and condition keys for Amazon Managed Workflows for Apache Airflow
- Actions, resources, and condition keys for AWS Marketplace
- Actions, resources, and condition keys for AWS Marketplace Catalog
- Actions, resources, and condition keys for AWS Marketplace Commerce Analytics Service
- Actions, resources, and condition keys for AWS Marketplace Deployment Service
- Actions, resources, and condition keys for AWS Marketplace Discovery
- Actions, resources, and condition keys for AWS Marketplace Entitlement Service
- Actions, resources, and condition keys for AWS Marketplace Image Building Service
- Actions, resources, and condition keys for AWS Marketplace Management Portal
- Actions, resources, and condition keys for AWS Marketplace Metering Service
- Actions, resources, and condition keys for AWS Marketplace Private Marketplace
- Actions, resources, and condition keys for AWS Marketplace Procurement Systems Integration
- Actions, resources, and condition keys for AWS Marketplace Reporting
- Actions, resources, and condition keys for AWS Marketplace Seller Reporting
- Actions, resources, and condition keys for AWS Marketplace Vendor Insights
- Actions, resources, and condition keys for AWS MCP Server
- Actions, resources, and condition keys for Amazon Mechanical Turk
- 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 AWS Microservice Extractor for .NET
- Actions, resources, and condition keys for AWS Migration Acceleration Program Credits
- Actions, resources, and condition keys for AWS Migration Hub
- Actions, resources, and condition keys for AWS Migration Hub Orchestrator
- Actions, resources, and condition keys for AWS Migration Hub Refactor Spaces
- Actions, resources, and condition keys for AWS Migration Hub Strategy Recommendations

- Actions, resources, and condition keys for Amazon Mobile Analytics
- Actions, resources, and condition keys for Amazon Monitron
- Actions, resources, and condition keys for Amazon MQ
- Actions, resources, and condition keys for Multi-party approval
- Actions, resources, and condition keys for AWS MWAA Serverless
- Actions, resources, and condition keys for Amazon Neptune
- Actions, resources, and condition keys for Amazon Neptune Analytics
- Actions, resources, and condition keys for AWS Network Firewall
- Actions, resources, and condition keys for Network Flow Monitor
- Actions, resources, and condition keys for AWS Network Manager
- Actions, resources, and condition keys for AWS Network Manager Chat
- Actions, resources, and condition keys for Amazon Nimble Studio
- Actions, resources, and condition keys for Amazon Nova Act
- Actions, resources, and condition keys for Amazon One Enterprise
- Actions, resources, and condition keys for Amazon OpenSearch
- Actions, resources, and condition keys for Amazon OpenSearch Ingestion
- Actions, resources, and condition keys for Amazon OpenSearch Serverless
- Actions, resources, and condition keys for Amazon OpenSearch Service
- Actions, resources, and condition keys for AWS OpsWorks
- Actions, resources, and condition keys for AWS OpsWorks Configuration Management
- Actions, resources, and condition keys for AWS Organizations
- Actions, resources, and condition keys for AWS Outposts
- Actions, resources, and condition keys for AWS Panorama
- Actions, resources, and condition keys for AWS Parallel Computing Service
- Actions, resources, and condition keys for AWS Partner Central
- Actions, resources, and condition keys for AWS Partner central account management
- Actions, resources, and condition keys for AWS Payment Cryptography
- Actions, resources, and condition keys for AWS Payments
- Actions, resources, and condition keys for AWS Performance Insights

- Actions, resources, and condition keys for Amazon Personalize
- Actions, resources, and condition keys for Amazon Pinpoint
- Actions, resources, and condition keys for Amazon Pinpoint Email Service
- Actions, resources, and condition keys for Amazon Pinpoint SMS and Voice Service
- Actions, resources, and condition keys for Amazon Polly
- Actions, resources, and condition keys for AWS Price List
- Actions, resources, and condition keys for AWS PricingPlanManager Service
- Actions, resources, and condition keys for AWS Private CA Connector for Active Directory
- Actions, resources, and condition keys for AWS Private CA Connector for SCEP
- Actions, resources, and condition keys for AWS Private Certificate Authority
- Actions, resources, and condition keys for AWS PrivateLink
- Actions, resources, and condition keys for AWS Proton
- Actions, resources, and condition keys for AWS Purchase Orders Console
- Actions, resources, and condition keys for Amazon Q
- Actions, resources, and condition keys for Amazon Q Business
- Actions, resources, and condition keys for Amazon Q Business Q Apps
- Actions, resources, and condition keys for Amazon Q Developer
- Actions, resources, and condition keys for Amazon Q in Connect
- Actions, resources, and condition keys for Amazon QLDB
- Actions, resources, and condition keys for Amazon QuickSight
- Actions, resources, and condition keys for Amazon RDS
- Actions, resources, and condition keys for Amazon RDS Data API
- Actions, resources, and condition keys for Amazon RDS IAM Authentication
- Actions, resources, and condition keys for AWS 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 Rekognition
- Actions, resources, and condition keys for AWS rePost Private

- Actions, resources, and condition keys for AWS Resilience Hub
- Actions, resources, and condition keys for AWS Resource Access Manager (RAM)
- Actions, resources, and condition keys for AWS Resource Explorer
- Actions, resources, and condition keys for Amazon Resource Group Tagging API
- Actions, resources, and condition keys for AWS Resource Groups
- Actions, resources, and condition keys for Amazon RHEL Knowledgebase Portal
- Actions, resources, and condition keys for AWS RoboMaker
- Actions, resources, and condition keys for Amazon Route 53
- Actions, resources, and condition keys for Amazon Route 53 Domains
- Actions, resources, and condition keys for Amazon Route 53 Profiles
- Actions, resources, and condition keys for Amazon Route 53 Recovery Cluster
- Actions, resources, and condition keys for Amazon Route 53 Recovery Controls
- Actions, resources, and condition keys for Amazon Route 53 Recovery Readiness
- Actions, resources, and condition keys for Amazon Route 53 Resolver
- Actions, resources, and condition keys for AWS Route53 Global Resolver
- Actions, resources, and condition keys for AWS RTB Fabric
- 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 S3 on Outposts
- Actions, resources, and condition keys for Amazon S3 Tables
- Actions, resources, and condition keys for Amazon S3 Vectors
- Actions, resources, and condition keys for Amazon SageMaker
- Actions, resources, and condition keys for Amazon SageMaker data science assistant
- Actions, resources, and condition keys for Amazon SageMaker geospatial capabilities
- Actions, resources, and condition keys for Amazon SageMaker Unified Studio MCP
- Actions, resources, and condition keys for Amazon SageMaker with MLflow
- Actions, resources, and condition keys for AWS Savings Plans

- Actions, resources, and condition keys for AWS Secrets Manager
- Actions, resources, and condition keys for AWS Security Agent
- Actions, resources, and condition keys for AWS Security Hub
- Actions, resources, and condition keys for AWS Security Incident Response
- Actions, resources, and condition keys for Amazon Security Lake
- Actions, resources, and condition keys for AWS Security Token Service
- Actions, resources, and condition keys for AWS Server Migration Service
- Actions, resources, and condition keys for AWS Serverless Application Repository
- Actions, resources, and condition keys for AWS Service - Oracle Database@AWS
- Actions, resources, and condition keys for AWS Service Catalog
- Actions, resources, and condition keys for AWS service providing managed private networks
- Actions, resources, and condition keys for Service Quotas
- Actions, resources, and condition keys for Amazon SES
- Actions, resources, and condition keys for AWS Shield
- Actions, resources, and condition keys for AWS Shield network security director
- Actions, resources, and condition keys for AWS Signer
- Actions, resources, and condition keys for AWS Signin
- Actions, resources, and condition keys for Amazon Simple Email Service - Mail Manager
- Actions, resources, and condition keys for Amazon Simple Email Service v2
- Actions, resources, and condition keys for Amazon Simple Workflow Service
- Actions, resources, and condition keys for Amazon SimpleDB
- Actions, resources, and condition keys for AWS SimSpace Weaver
- Actions, resources, and condition keys for AWS Snow Device Management
- Actions, resources, and condition keys for AWS Snowball
- Actions, resources, and condition keys for Amazon SNS
- Actions, resources, and condition keys for AWS SQL Workbench
- Actions, resources, and condition keys for Amazon SQS
- Actions, resources, and condition keys for AWS Step Functions
- Actions, resources, and condition keys for AWS Storage Gateway

- Actions, resources, and condition keys for AWS Supply Chain
- Actions, resources, and condition keys for AWS Support
- Actions, resources, and condition keys for AWS Support App in Slack
- Actions, resources, and condition keys for AWS Support Console
- Actions, resources, and condition keys for AWS Support Plans
- Actions, resources, and condition keys for AWS Sustainability
- Actions, resources, and condition keys for AWS Systems Manager
- Actions, resources, and condition keys for AWS Systems Manager for SAP
- Actions, resources, and condition keys for AWS Systems Manager GUI Connect
- Actions, resources, and condition keys for AWS Systems Manager Incident Manager
- Actions, resources, and condition keys for AWS Systems Manager Incident Manager Contacts
- Actions, resources, and condition keys for AWS Systems Manager Quick Setup
- Actions, resources, and condition keys for Tag Editor
- Actions, resources, and condition keys for AWS Tax Settings
- Actions, resources, and condition keys for AWS Telco Network Builder
- Actions, resources, and condition keys for Amazon Textract
- Actions, resources, and condition keys for Amazon Timestream
- Actions, resources, and condition keys for Amazon Timestream InfluxDB
- Actions, resources, and condition keys for AWS Tiros
- Actions, resources, and condition keys for Amazon Transcribe
- Actions, resources, and condition keys for AWS Transfer Family
- Actions, resources, and condition keys for AWS Transform
- Actions, resources, and condition keys for AWS Transform custom
- Actions, resources, and condition keys for Amazon Translate
- Actions, resources, and condition keys for AWS Trusted Advisor
- Actions, resources, and condition keys for AWS User Experience Customization
- Actions, resources, and condition keys for AWS User Notifications
- Actions, resources, and condition keys for AWS User Notifications Contacts
- Actions, resources, and condition keys for AWS User Subscriptions

- Actions, resources, and condition keys for AWS Verified Access
- Actions, resources, and condition keys for Amazon Verified Permissions
- Actions, resources, and condition keys for Amazon VPC Lattice
- Actions, resources, and condition keys for Amazon VPC Lattice Services
- Actions, resources, and condition keys for AWS WAF
- Actions, resources, and condition keys for AWS WAF Regional
- Actions, resources, and condition keys for AWS WAF V2
- Actions, resources, and condition keys for AWS Well-Architected Tool
- Actions, resources, and condition keys for AWS Wickr
- Actions, resources, and condition keys for Amazon WorkDocs
- Actions, resources, and condition keys for Amazon WorkLink
- Actions, resources, and condition keys for Amazon WorkMail
- Actions, resources, and condition keys for Amazon WorkMail Message Flow
- Actions, resources, and condition keys for Amazon WorkSpaces
- Actions, resources, and condition keys for Amazon WorkSpaces Application Manager
- Actions, resources, and condition keys for AWS WorkSpaces Managed Instances
- Actions, resources, and condition keys for Amazon WorkSpaces Secure Browser
- Actions, resources, and condition keys for Amazon WorkSpaces Thin Client
- Actions, resources, and condition keys for AWS X-Ray

Actions, resources, and condition keys for AWS Account Management

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

References:

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

Topics

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

Actions defined by AWS Account Management

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

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

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

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

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

Note

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

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

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

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

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

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

Resource types defined by AWS Account Management

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

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

Condition keys for AWS Account Management

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

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

Condition keys	Description	Type
account:AccountResourceOrgPaths	Filters access by the resource path for an account in an organization	ArrayOfString
account:AccountRes	Filters access by resource tags for an account in an organization	String

Condition keys	Description	Type
ourceOrgTags/${TagKey}		
account:AlternateContactTypes	Filters access by alternate contact types	ArrayOfString
account:EmailTargetDomain	Filters access by email domain of the target email address	String
account:TargetRegion	Filters access by a list of Regions. Enables or disables all the Regions specified here	String

Actions, resources, and condition keys for AWS Action Recommendations

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

References:

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

Topics

- Actions defined by AWS Action Recommendations
- Resource types defined by AWS Action Recommendations
- Condition keys for AWS Action Recommendations

Actions defined by AWS Action Recommendations

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecommendedActions	Grants permission to list recommended actions in the AWS Management Console	List			

Resource types defined by AWS Action Recommendations

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

Condition keys for AWS Action Recommendations

Action Recommendations has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Activate

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

References:

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

Topics

Actions defined by AWS Activate

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateForm	Grants permission to submit an Activate application form	Write			
GetAccountContact	Grants permission to get the AWS account contact information	Read			
GetContentInfo	Grants permission to get Activate tech posts and offer information	Read			
GetCosts	Grants permission to get the AWS cost information	Read			
GetCredits	Grants permission to get the AWS credit information	Read			
GetMemberInfo	Grants permission to get the Activate member information	Read			
GetProgram	Grants permission to get an Activate program	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMemberInfo	Grants permission to create or update the Activate member information	Write			

Resource types defined by AWS Activate

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

Condition keys for AWS Activate

Activate has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon AI Operations

Amazon AI Operations (service prefix: `aiops`) 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 AI Operations
- Resource types defined by Amazon AI Operations
- Condition keys for Amazon AI Operations

Actions defined by Amazon AI Operations

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInvestigation	Grants permission to create a new investigation in the specified investigation group	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
CreateInvestigationEvent	Grants permission to create a new investigation event in the specified investigation group	Write	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:Decrypt kms:GenerateDataKey logs:GetQueryResults sts:SetContext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInvestigationGroup	Grants permission to create a new investigation group	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	aiops:TagResource cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInvestigationResource	Grants permission to create an investigation resource in the specified investigation group	Write	investigation-group*		cloudwatch:DescribeAlarmHistory cloudwatch:DescribeAlarms cloudwatch:GetInsightRuleReport cloudwatch:GetMetricData kms:GenerateDataKey logs:GetQueryResults

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReport	Grants permission to create a new report in the specified investigation	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
DeleteInvestigation	Grants permission to delete an investigation in the specified investigation group	Write	investigation-group*		sts:SetContext
DeleteInvestigationGroup	Grants permission to delete the specified investigation group	Write	investigation-group*		sso:DeleteApplication
DeleteInvestigationGroupPolicy	Grants permission to delete the investigation group policy attached to an investigation group	Write	investigation-group*		
GenerateReport	Grants permission to generate a report in the specified investigation report	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEphemeralInvestigationResults	Grants permission to run and retrieve ephemeral investigation results	List			
GetFact	Grants permission to retrieve a fact in the specified investigation report	Read	investigation-group*		kms:Decrypt
GetFactVersions	Grants permission to retrieve all versions of a fact token in the specified investigation report	Read	investigation-group*		kms:Decrypt
GetInvestigation	Grants permission to retrieve an investigation in the specified investigation group	Read	investigation-group*		
GetInvestigationEvent	Grants permission to retrieve an investigation event in the specified investigation group	Read	investigation-group*		kms:Decrypt
GetInvestigationGroup	Grants permission to retrieve the specified investigation group	Read	investigation-group*		
GetInvestigationGroupPolicy	Grants permission to retrieve the investigation group policy attached to an investigation group	Read	investigation-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInvestigationResource	Grants permission to retrieve an investigation resource in the specified investigation group	Read	investigation-group*		kms:Decrypt
GetReport	Grants permission to retrieve a report in the specified investigation	Read	investigation-group*		kms:Decrypt
ListFacts	Grants permission to list all facts in the specified investigation report	List	investigation-group*		kms:Decrypt
ListInvestigationEvents	Grants permission to list all investigation events in the specified investigation group	List	investigation-group*		
ListInvestigationGroups	Grants permission to list all investigation groups in the AWS account making the request	List			
ListInvestigations	Grants permission to list all investigations that are in the specified investigation group	List	investigation-group*		
ListReports	Grants permission to list all reports in the specified investigation	List	investigation-group*		
ListTagsForResource	Grants permission to list the tags for the specified resource	List	investigation-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFact	Grants permission to create or update a new fact in the specified investigation report	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
PutInvestigationGroupPolicy	Grants permission to create/update the investigation group policy attached to an investigation group	Write	investigation-group*		
TagResource	Grants permission to add or update the specified tags for the specified resource	Tagging	investigation-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	investigation-group*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInvestigation	Grants permission to update an investigation in the specified investigation group	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
UpdateInvestigationEvent	Grants permission to update an investigation event in the specified investigation group	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInvestigationGroup	Grants permission to update the specified investigation group	Write	investigation-group*		cloudtrail:DescribeTrails iam:PassRole kms:Decrypt kms:DescribeKey kms:GenerateDataKey sso:CreateApplication sso:DeleteApplication sso:PutApplicationAccessScope sso:PutApplicationAssignmen

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					tConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant sso:TagResource
UpdateReport	Grants permission to update a report in the specified investigation	Write	investigation-group*		kms:Decrypt kms:GenerateDataKey sts:SetContext
ValidateInvestigationGroup	Grants permission to validate the specified investigation group	Read	investigation-group*		

Resource types defined by Amazon AI Operations

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
investigation-group	`arn:${Partition}:aiops:${Region}:${Account}:investigation-group/${InvestigationGroupId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon AI Operations

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

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

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

Actions, resources, and condition keys for Alexa for Business

Alexa for Business (service prefix: a4b) 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 Alexa for Business

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApproveSkill	Grants permission to associate a skill with the organization under the customer's AWS account	Write			
AssociateContactWithAddressBook	Grants permission to associate a contact with a given address book	Write	addressbook*		
			contact*		
AssociateDeviceWit	Grants permission to associate a device with the specified network profile	Write	device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
hNetworkProfile			networkprofile*		
AssociateDeviceWithRoom	Grants permission to associate device with given room	Write	device* room*		
AssociateSkillGroupWithRoom	Grants permission to associate the skill group with given room	Write	room* skillgroup*		
AssociateSkillWithSkillGroup	Grants permission to associate a skill with a skill group	Write	skillgroup*		
AssociateSkillWithUsers	Grants permission to make a private skill available for enrolled users to enable on their devices	Write			
CompleteRegistration [permission only]	Grants permission to complete the operation of registering an Alexa device	Write			
CreateAddressBook	Grants permission to create an address book with the specified details	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBusinessReportSchedule	Grants permission to create a recurring schedule for usage reports to deliver to the specified S3 location with a specified daily or weekly interval	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConferenceProvider	Grants permission to add a new conference provider under the user's AWS account	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContact	Grants permission to create a contact with the specified details	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGatewayGroup	Grants permission to create a gateway group with the specified details	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkProfile	Grants permission to create a network profile with the specified details	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Grants permission to create a new profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoom	Grants permission to create room with the specified details	Write	profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSkillGroup	Grants permission to create a skill group with given name and description	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser	Grants permission to create a user	Write	user*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddressBook	Grants permission to delete an address book by the address book ARN	Write	addressbook*		
DeleteBusinessReportSchedule	Grants permission to delete the recurring report delivery schedule with the specified schedule ARN	Write	schedule*		
DeleteConferenceProvider	Grants permission to delete a conference provider	Write	conferenceprovider*		
DeleteContact	Grants permission to delete a contact by the contact ARN	Write	contact*		
DeleteDevice	Grants permission to remove a device from Alexa For Business	Write	device*		
DeleteDeviceUsageData	Grants permission to delete the device's entire previous history of voice input data and associated response data	Write	device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGatewayGroup	Grants permission to delete a gateway group	Write	gatewaygroup*		
DeleteNetworkProfile	Grants permission to delete a network profile by the network profile ARN	Write	networkprofile*		
DeleteProfile	Grants permission to delete profile by profile ARN	Write	profile*		
DeleteRoom	Grants permission to delete room	Write	room*		
DeleteRoomSkillParameter	Grants permission to delete a parameter from a skill and room	Write	room*		
DeleteSkillAuthorization	Grants permission to unlink a third-party account from a skill	Write	room*		
DeleteSkillGroup	Grants permission to delete skill group with skill group ARN	Write	skillgroup*		
DeleteUser	Grants permission to delete a user	Write	user*		
DisassociateContactFromAddressBook	Grants permission to disassociate a contact from a given address book	Write	addressbook*		
			contact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateDeviceFromRoom	Grants permission to disassociate device from its current room	Write	device*		
DisassociateSkillFromSkillGroup	Grants permission to disassociate a skill from a skill group	Write	skillgroup*		
DisassociateSkillFromUsers	Grants permission to make a private skill unavailable for enrolled users and prevent them from enabling it on their devices	Write	user*		
DisassociateSkillGroupFromRoom	Grants permission to disassociate the skill group from given room	Write	room* skillgroup*		
ForgetSmartHomeAppliances	Grants permission to forget smart home appliances associated to a room	Write	room*		
GetAddressBook	Grants permission to get the address book details by the address book ARN	Read	addressbook*		
GetConferencePreference	Grants permission to retrieve the existing conference preferences	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConferenceProvider	Grants permission to get details about a specific conference provider	Read	conferenceprovider*		
GetContact	Grants permission to get the contact details by the contact ARN	Read	contact*		
GetDevice	Grants permission to get device details	Read	device*		
GetGateway	Grants permission to retrieve the details of a gateway	Read	gateway*		
GetGatewayGroup	Grants permission to retrieve the details of a gateway group	Read	gatewaygroup*		
GetInvitationConfiguration	Grants permission to retrieve the configured values for the user enrollment invitation email template	Read			
GetNetworkProfile	Grants permission to get the network profile details by the network profile ARN	Read	networkprofile*		
GetProfile	Grants permission to get profile when provided with Profile ARN	Read	profile*		
GetRoom	Grants permission to get room details	Read	room*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRoomSkillParameter	Grants permission to get an existing parameter that has been set for a skill and room	Read	room*		
GetSkillGroup	Grants permission to get skill group details with skill group ARN	Read	skillgroup*		
ListBusinessReportSchedules	Grants permission to list the details of the schedules that a user configured	List			
ListConferenceProviders	Grants permission to list conference providers under a specific AWS account	List			
ListDeviceEvents	Grants permission to list the device event history, including device connection status, for up to 30 days	List	device*		
ListGatewayGroups	Grants permission to list gateway group summaries	List			
ListGateways	Grants permission to list gateway summaries	List	gatewaygroup*		
ListSkills	Grants permission to list skills	List			
ListSkillsStoreCategories	Grants permission to list all categories in the Alexa skill store	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSkillsStoreSkillsByCategory	Grants permission to list all skills in the Alexa skill store by category	List			
ListSmartHomeAppliances	Grants permission to list all of the smart home appliances associated with a room	List	room*		
ListTags	Grants permission to list all tags on a resource	Read	device		
			room		
			user		
PutConferencePreference	Grants permission to set the conference preferences on a specific conference provider at the account level	Write			
PutDeviceSetupEvents [permission only]	Grants permission to publish Alexa device setup events	Write			
PutInvitationConfiguration	Grants permission to configure the email template for the user enrollment invitation with the specified attributes	Write			
PutRoomSkillParameter	Grants permission to put a room specific parameter for a skill	Write	room*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutSkillAuthorization	Grants permission to link a user's account to a third-party skill provider	Write	room*		
RegisterAVSDevice	Grants permission to register an Alexa-enabled device built by an Original Equipment Manufacturer (OEM) using Alexa Voice Service (AVS)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterDevice [permission only]	Grants permission to register an Alexa device	Write			
RejectSkill	Grants permission to disassociate a skill from the organization under a user's AWS account	Write			
ResolveRoom	Grants permission to resolve room information	Read			
RevokeInvitation	Grants permission to revoke an invitation	Write	user*		
SearchAddressBooks	Grants permission to search address books and list the ones that meet a set of filter and sort criteria	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchContacts	Grants permission to search contacts and list the ones that meet a set of filter and sort criteria	List			
SearchDevices	Grants permission to search for devices	List			
SearchNetworkProfiles	Grants permission to search network profiles and list the ones that meet a set of filter and sort criteria	List			
SearchProfiles	Grants permission to search for profiles	List			
SearchRooms	Grants permission to search for rooms	List			
SearchSkillGroups	Grants permission to search for skill groups	List			
SearchUsers	Grants permission to search for users	List			
SendAnnouncement	Grants permission to trigger an asynchronous flow to send text, SSML, or audio announcements to rooms that are identified by a search or filter	Write			
SendInvitation	Grants permission to send an invitation to a user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDeviceSync	Grants permission to restore the device and its account to its known, default settings by clearing all information and settings set by its previous users	Write			
StartSmartHomeApplianceDiscovery	Grants permission to initiate the discovery of any smart home appliances associated with the room	Read	room*		
TagResource	Grants permission to add metadata tags to a resource	Tagging	device		
			room		
			user		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove metadata tags from a resource	Tagging	device		
			room		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAddressBook	Grants permission to update address book details by the address book ARN	Write	addressbook*		
UpdateBusinessReportSchedule	Grants permission to update the configuration of the report delivery schedule with the specified schedule ARN	Write	schedule*		
UpdateConferenceProvider	Grants permission to update an existing conference provider's settings	Write	conferenceprovider*		
UpdateContact	Grants permission to update the contact details by the contact ARN	Write	contact*		
UpdateDevice	Grants permission to update device name	Write	device*		
UpdateGateway	Grants permission to update the details of a gateway	Write	gateway*		
UpdateGatewayGroup	Grants permission to update the details of a gateway group	Write	gatewaygroup*		
UpdateNetworkProfile	Grants permission to update a network profile by the network profile ARN	Write	networkprofile*		
UpdateProfile	Grants permission to update an existing profile	Write	profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRoom	Grants permission to update room details	Write	room*		
UpdateSkillGroup	Grants permission to update skill group details with skill group ARN	Write	skillgroup*		

Resource types defined by Alexa for Business

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:${Partition}:a4b:${Region}:${Account}:profile/${ResourceId}`	
room	`arn:${Partition}:a4b:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:a4b:${Region}:${Account}:device/${ResourceId}`	aws:ResourceTag/${TagKey}
skillgroup	`arn:${Partition}:a4b:${Region}:${Account}:skill-group/${ResourceId}`	
user	`arn:${Partition}:a4b:${Region}:${Account}:user/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
addressbook	arn:${Partition}:a4b:${Region}:${Account}:address-book/${ResourceId}	
conferenceprovider	arn:${Partition}:a4b:${Region}:${Account}:conference-provider/${ResourceId}	
contact	arn:${Partition}:a4b:${Region}:${Account}:contact/${ResourceId}	
schedule	arn:${Partition}:a4b:${Region}:${Account}:schedule/${ResourceId}	
networkprofile	arn:${Partition}:a4b:${Region}:${Account}:network-profile/${ResourceId}	
gateway	arn:${Partition}:a4b:${Region}:${Account}:gateway/${ResourceId}	
gatewaygroup	arn:${Partition}:a4b:${Region}:${Account}:gateway-group/${ResourceId}	

Condition keys for Alexa for Business

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

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

Condition keys	Description	Type
a4b:amazonId	Filters actions based on the Amazon Id in the request	String

Condition keys	Description	Type
a4b:filters_deviceType	Filters actions based on the device type in the request	ArrayOfString
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 AmazonMediaImport

AmazonMediaImport (service prefix: `mediaimport`) 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 AmazonMediaImport
- Resource types defined by AmazonMediaImport
- Condition keys for AmazonMediaImport

Actions defined by AmazonMediaImport

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDatabaseBinarySnapshot [permission only]	Grants permission to create a database binary snapshot on the customer's aws account	Write			

Resource types defined by AmazonMediaImport

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

Condition keys for AmazonMediaImport

mediaimport has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Amplify

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

References:

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

Topics

- Actions defined by AWS Amplify

- Resource types defined by AWS Amplify
- Condition keys for AWS Amplify

Actions defined by AWS Amplify

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateWebACL	Grants permission to associate a WebACL to a Resource	Write	apps*		
CreateApp	Grants permission to create a new Amplify App	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBackendEnvironment	Grants permission to create a new backend environment for an Amplify App	Write	apps*		
CreateBranch	Grants permission to create a new Branch for an Amplify App	Write	branches*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateDeployment	Grants permission to create a deployment for manual deploy apps. (Apps are not connected to repository)	Write	branches*		
CreateDomainAssociation	Grants permission to create a new DomainAssociation on an App	Write	domains*		
CreateWebHook	Grants permission to create a new webhook on an App	Write	branches*		
DeleteApp	Grants permission to delete an existing Amplify App by appId	Write	apps*		
DeleteBackendEnvironment	Grants permission to delete a branch for an Amplify App	Write	apps*		
DeleteBranch	Grants permission to delete a branch for an Amplify App	Write	branches*		
DeleteDomainAssociation	Grants permission to delete a DomainAssociation	Write	domains*		
DeleteJob	Grants permission to delete a job, for an Amplify branch, part of Amplify App	Write	jobs*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWebHook	Grants permission to delete a webhook by id	Write	webhooks*		
DisassociateWebACL	Grants permission to disassociate a WebACL from a Resource	Write	apps*		
GenerateAccessLogs	Grants permission to generate website access logs for a specific time range via a pre-signed URL	Write	apps*		
GetApp	Grants permission to retrieve an existing Amplify App by appId	Read	apps*		
GetArtifactUrl	Grants permission to retrieve artifact info that corresponds to a artifactId	Read	apps*		
GetBackendEnvironment	Grants permission to retrieve a backend environment for an Amplify App	Read	apps*		
GetBranch	Grants permission to retrieve a branch for an Amplify App	Read	branches*		
GetDomainAssociation	Grants permission to retrieve domain info that corresponds to an appId and domainName	Read	domains*		
GetJob	Grants permission to get a job for a branch, part of an Amplify App	Read	jobs*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWebACLForResource	Grants permission to retrieve the WebACL associated with a Resource	Read	apps*		
GetWebHook	Grants permission to retrieve webhook info that corresponds to a webhookId	Read	webhooks*		
ListApps	Grants permission to list existing Amplify Apps	List			
ListArtifacts	Grants permission to list artifacts with an app, a branch, a job and an artifact type	List	apps*		
ListBackendEnvironments	Grants permission to list backend environments for an Amplify App	List	apps*		
ListBranches	Grants permission to list branches for an Amplify App	List	apps*		
ListDomainAssociations	Grants permission to list domains with an app	List	apps*		
ListJobs	Grants permission to list Jobs for a branch, part of an Amplify App	List	branches*		
ListResourcesForWebACL	Grants permission to list the Resources associated with a WebACL	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for an AWS Amplify Console resource	Read	apps		
			branches		
			domains		
			webhooks		
ListWebHooks	Grants permission to list webhooks on an App	List	apps*		
StartDeployment	Grants permission to start a deployment for manual deploy apps. (Apps are not connected to repository)	Write	branches*		
StartJob	Grants permission to start a new job for a branch, part of an Amplify App	Write	jobs*		
StopJob	Grants permission to stop a job that is in progress, for an Amplify branch, part of Amplify App	Write	jobs*		
TagResource	Grants permission to tag an AWS Amplify Console resource	Tagging	apps		
			branches		
			domains		
			webhooks		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag from an AWS Amplify Console resource	Tagging	apps		
			branches		
			domains		
			webhooks		
				aws:TagKeys	
UpdateApp	Grants permission to update an existing Amplify App	Write	apps*		
UpdateBranch	Grants permission to update a branch for an Amplify App	Write	branches*		
UpdateDomainAssociation	Grants permission to update a DomainAssociation on an App	Write	domains*		
UpdateWebHook	Grants permission to update a webhook	Write	webhooks*		

Resource types defined by AWS Amplify

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
apps	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
branches	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}`	aws:ResourceTag/${TagKey}
jobs	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/branches/${BranchName}/jobs/${JobId}`	
domains	`arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}/domains/${DomainName}`	aws:ResourceTag/${TagKey}
webhooks	`arn:${Partition}:amplify:${Region}:${Account}:webhooks/${WebhookId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Amplify

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

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

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

Actions, resources, and condition keys for AWS Amplify Admin

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

References:

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

Topics

- Actions defined by AWS Amplify Admin
- Resource types defined by AWS Amplify Admin
- Condition keys for AWS Amplify Admin

Actions defined by AWS Amplify Admin

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CloneBackend	Grants permission to clone an existing Amplify Admin backend environment into a new Amplify Admin backend enviroment	Write	backend*		
CreateBackend	Grants permission to create a new Amplify Admin backend environment by Amplify appId	Write	created-backend*		
CreateBackendAPI	Grants permission to create an API for an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api* backend* environment*		
CreateBackendAuth	Grants permission to create an auth resource for an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth* backend* environment*		
CreateBackendConfig	Grants permission to create a new Amplify Admin backend config by Amplify appId	Write	config*		
CreateBackendStorage	Grants permission to create a backend storage resource	Write	backend* environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			storage*		
CreateToken	Grants permission to create an Amplify Admin challenge token by appId	Write	backend*		
			token*		
DeleteBackend	Grants permission to delete an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	backend*		
			environment*		
DeleteBackendAPI	Grants permission to delete an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api*		
			backend*		
			environment*		
DeleteBackendAuth	Grants permission to delete an auth resource of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth*		
			backend*		
			environment*		
DeleteBackendStorage	Grants permission to delete a backend storage resource	Write	backend*		
			environment*		
			storage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteToken	Grants permission to delete an Amplify Admin challenge token by appId	Write	backend*		
			token*		
GenerateBackendAPIModels	Grants permission to generate models for an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api*		
			backend*		
			environment*		
GetBackend	Grants permission to retrieve an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	backend*		
			environment*		
GetBackendAPI	Grants permission to retrieve an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	api*		
			backend*		
			environment*		
GetBackendAPIModels	Grants permission to retrieve models for an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	api*		
			backend*		
			environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBackendAuth	Grants permission to retrieve an auth resource of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	auth*		
			backend*		
			environment*		
GetBackendJob	Grants permission to retrieve a job of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Read	backend*		
			job*		
GetBackendStorage	Grants permission to retrieve an existing backend storage resource	Read	backend*		
			environment*		
GetToken	Grants permission to retrieve an Amplify Admin challenge token by appId	Read	backend*		
			token*		
ImportBackendAuth	Grants permission to import an existing auth resource of an Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth*		
			backend*		
			environment*		
ImportBackendStorage	Grants permission to import an existing backend storage resource	Write	backend*		
			environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			storage*		
ListBackendJobs	Grants permission to retrieve the jobs of an existing Amplify Admin backend environment by appId and backendEnvironmentName	List	backend*		
			job*		
ListS3Buckets	Grants permission to retrieve s3 buckets	List			s3:ListAllMyBuckets
RemoveAllBackends	Grants permission to delete all existing Amplify Admin backend environments by appId	Write	backend*		
			environment*		
RemoveBackendConfig	Grants permission to delete an Amplify Admin backend config by Amplify appId	Write	config*		
UpdateBackendAPI	Grants permission to update an API of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	api*		
			backend*		
			environment*		
UpdateBackendAuth	Grants permission to update an auth resource of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	auth*		
			backend*		
			environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBackendConfig	Grants permission to update an Amplify Admin backend config by Amplify appId	Write	config*		
UpdateBackendJob	Grants permission to update a job of an existing Amplify Admin backend environment by appId and backendEnvironmentName	Write	backend*		
			job*		
UpdateBackendStorage	Grants permission to update a backend storage resource	Write	backend*		
			environment*		
			storage*		

Resource types defined by AWS Amplify Admin

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
created-backend	`arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/*`	

Resource types	ARN	Condition keys
backend	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/*	
environment	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/environments/*	
api	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/api/*	
auth	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/auth/*	
job	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/job/*	
config	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/config/*	
token	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/challenge/*	
storage	arn:${Partition}:amplifybackend:${Region}:${Account}:/backend/${AppId}/storage/*	

Condition keys for AWS Amplify Admin

Amplify Admin has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Amplify UI Builder

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

References:

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

Topics

- Actions defined by AWS Amplify UI Builder
- Resource types defined by AWS Amplify UI Builder
- Condition keys for AWS Amplify UI Builder

Actions defined by AWS Amplify UI Builder

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateComponent	Grants permission to create a component	Write		aws:RequestTag/${TagKey}	amplify:GetApp amplifyuibuilder:G

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	etComponent amplifyuibuilder:TagResource
CreateForm	Grants permission to create a form	Write		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTheme	Grants permission to create a theme	Write		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource
DeleteComponent	Grants permission to delete a component	Write	Component Resource*		amplify:GetApp amplifyuibuilder:UntagResource
DeleteForm	Grants permission to delete a form	Write	FormResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTheme	Grants permission to delete a theme	Write	ThemeResource*		amplify:GetApp amplifyuibuilder:UntagResource
ExchangeCodeForToken	Grants permission to exchange a code for a token	Write			
ExportComponents	Grants permission to export components	Read			
ExportForms	Grants permission to export forms	Read			
ExportThemes	Grants permission to export themes	Read			
GetCodegenJob	Grants permission to get an existing codegen job	Read	CodegenJobResource*		amplify:GetApp
GetComponent	Grants permission to get an existing component	Read	ComponentResource*		amplify:GetApp
GetForm	Grants permission to get an existing form	Read	FormResource*		amplify:GetApp
GetMetadata	Grants permission to get an existing metadata	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTheme	Grants permission to get an existing theme	Read	ThemeResource*		amplify:GetApp
ListCodegenJobs	Grants permission to list codegen jobs	List			amplify:GetApp
ListComponents	Grants permission to list components	List			amplify:GetApp
ListForms	Grants permission to list forms	List			amplify:GetApp
ListTagsForResource	Grants permission to list tags for a specified Amazon Resource Name (ARN)	List	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
ListThemes	Grants permission to list themes	List			amplify:GetApp
PutMetadataFlag	Grants permission to put an existing metadata	Write			
RefreshToken	Grants permission to refresh an access token	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetMetadataFlag	Grants permission to reset an existing metadata	Write			
StartCodegenJob	Grants permission to start a codegen job	Write		aws:RequestTag/${TagKey} aws:TagKeys	amplify:GetApp
TagResource	Grants permission to tag the resource with a tag key and value	Tagging	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag a resource with a specified Amazon Resource Name (ARN)	Tagging	CodegenJobResource		
			ComponentResource		
			FormResource		
			ThemeResource		
				aws:TagKeys	
UpdateComponent	Grants permission to update a component	Write	ComponentResource*		amplify:GetApp amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateForm	Grants permission to update a form	Write	FormResource*		amplify:GetApp amplifyuibuilder:GetForm amplifyuibuilder:TagResource amplifyuibuilder:UntagResource
UpdateTheme	Grants permission to update a theme	Write	ThemeResource*		amplify:GetApp amplifyuibuilder:GetTheme amplifyuibuilder:TagResource amplifyuibuilder:UntagResource

Resource types defined by AWS Amplify UI 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
CodegenJobResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/codegen-jobs/${Id}`	amplifyuibuilder:CodegenJobResourceAppId amplifyuibuilder:CodegenJobResourceEnvironmentName amplifyuibuilder:CodegenJobResourceId aws:ResourceTag/${TagKey}
ComponentResource	`arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/components/${Id}`	amplifyuibuilder:ComponentResourceAppId amplifyuibuilder:ComponentResourceEnvironmentName amplifyuibuilder:ComponentResourceId aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
FormResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/forms/${Id}	amplifyuibuilder:FormResourceAppId amplifyuibuilder:FormResourceEnvironmentName amplifyuibuilder:FormResourceId aws:ResourceTag/${TagKey}
ThemeResource	arn:${Partition}:amplifyuibuilder:${Region}:${Account}:app/${AppId}/environment/${EnvironmentName}/themes/${Id}	amplifyuibuilder:ThemeResourceAppId amplifyuibuilder:ThemeResourceEnvironmentName amplifyuibuilder:ThemeResourceId aws:ResourceTag/${TagKey}

Condition keys for AWS Amplify UI Builder

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

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

Condition keys	Description	Type
amplifyuibuilder:CodegenJobResourceAppId	Filters access by the app ID	String
amplifyuibuilder:CodegenJobResourceEnvironmentName	Filters access by the backend environment name	String
amplifyuibuilder:CodegenJobResourceId	Filters access by the codegen job ID	String
amplifyuibuilder:ComponentResourceAppId	Filters access by the app ID	String
amplifyuibuilder:ComponentResourceEnvironmentName	Filters access by the backend environment name	String
amplifyuibuilder:ComponentResourceId	Filters access by the component ID	String
amplifyuibuilder:F	Filters access by the app ID	String

Condition keys	Description	Type
ormResourceAppId		
amplifyuibuilder:FormResourceEnvironmentName	Filters access by the backend environment name	String
amplifyuibuilder:FormResourceId	Filters access by the form ID	String
amplifyuibuilder:ThemeResourceAppId	Filters access by the app ID	String
amplifyuibuilder:ThemeResourceEnvironmentName	Filters access by the backend environment name	String
amplifyuibuilder:ThemeResourceId	Filters access by the theme 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

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

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AlterCluster	Grants permission to alter various aspects of the cluster, equivalent to Apache Kafka's ALTER CLUSTER ACL	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster

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 AWS global condition context keys.

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

Actions, resources, and condition keys for 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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvalidateCache	Grants permission to invalidate API cache upon a client request	Write	execute-api-general*		
Invoke	Grants permission to invoke an API upon a client request	Write	execute-api-domain		
			execute-api-general		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ManageConnections	Grants permission to access the Websocket @connections Route	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 AWS global condition context keys.

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

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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			DocumentationVersion		
			DomainName		
			DomainNameAccessAssociation		
			GatewayResponse		
			Integration		
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			PrivateBasePathMapping		
			PrivateDomainName		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			RequestValidator		
			Resource		
			RestApi		
			Stage		
			Tags		
			Template		
			UsagePlan		
			UsagePlanKey		
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
GET	Grants permission to read a particular resource	Read	Account		
			ApiKey		
			ApiKeys		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Authorizer		
			Authorizers		
			BasePathMapping		
			BasePathMappings		
			ClientCertificate		
			ClientCertificates		
			Deployment		
			Deployments		
			DocumentationPart		
			DocumentationParts		
			DocumentationVersion		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			DocumentationVersions		
			DomainName		
			DomainNameAccessAssociations		
			DomainNames		
			GatewayResponse		
			GatewayResponses		
			Integration		
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Models		
			PrivateBasePathMapping		
			PrivateBasePathMappings		
			PrivateDomainName		
			RequestValidator		
			RequestValidators		
			Resource		
			Resources		
			RestApi		
			RestApis		
			Sdk		
			Stage		
			Stages		
			Tags		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			UsagePlan		
			UsagePlanKey		
			UsagePlanKeys		
			UsagePlans		
			VpcLink		
			VpcLinks		
PATCH	Grants permission to update a particular resource	Write	Account		
			ApiKey		
			Authorizer		
			BasePathMapping		
			ClientCertificate		
			Deployment		
			DocumentationPart		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			DocumentationVersion		
			DomainName		
			GatewayResponse		
			Integration		
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			PrivateBasePathMapping		
			PrivateDomainName		
			RequestValidator		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Resource		
			RestApi		
			Stage		
			Template		
			UsagePlan		
			UsagePlanKey		
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
POST	Grants permission to create a particular resource	Write	ApiKeys		
			Authorizers		
			BasePathMappings		
			ClientCertificates		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Deployments		
			DocumentationParts		
			DocumentationVersions		
			DomainNameAccessAssociations		
			DomainNames		
			GatewayResponses		
			IntegrationResponse		
			MethodResponse		
			Models		
			PrivateBasePathMappings		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			RequestValidators		
			Resources		
			RestApis		
			Stages		
			UsagePlanKeys		
			UsagePlans		
			VpcLinks		
				aws:RequestTag/${TagKey} aws:TagKeys	
PUT	Grants permission to update a particular resource	Write	DocumentationPart		
			GatewayResponse		
			IntegrationResponse		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
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/${AuthorizerId}	apigateway:Request/AuthorizerType apigateway:Resource/AuthorizerType aws:ResourceTag/${TagKey}
Authorizers	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/authorizers	apigateway:Request/AuthorizerType aws:ResourceTag/${TagKey}
BasePathMapping	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/basepathmappings/${BasePath}	aws:ResourceTag/${TagKey}
BasePathMappings	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/basepathmappings	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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}
DocumentationVersions	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/versions	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
DomainName	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}	apigateway:Request/EndpointType apigateway:Request/MtlsTrustStoreUri apigateway:Request/MtlsTrustStoreVersion apigateway:Request/SecurityPolicy apigateway:Resource/EndpointType apigateway:Resource/MtlsTrustStoreUri apigateway:Resource/MtlsTrustStoreVersion apigateway:Resource/RoutingMode apigateway:Resource/SecurityPolicy aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
DomainNames	arn:${Partition}:apigateway:${Region}::/domainnames	apigateway:Request/EndpointType apigateway:Request/MtlsTrustStoreUri apigateway:Request/MtlsTrustStoreVersion apigateway:Request/SecurityPolicy apigateway:Resource/RoutingMode 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}

Resource types	ARN	Condition keys
GatewayResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/gatewayresponses/${ResponseType}	aws:ResourceTag/${TagKey}
GatewayResponses	arn:${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 apigateway:Resource/RoutingMode 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/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Request/SecurityPolicy apigateway:Resource/ApiKeyRequired apigateway:Resource/ApiName apigateway:Resource/AuthorizerType apigateway:Resource/DisableExecuteApiEndpoint

Resource types	ARN	Condition keys
		apigateway:Resource/EndpointType apigateway:Resource/RouteAuthorizationType apigateway:Resource/SecurityPolicy 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/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Request/SecurityPolicy 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 AWS 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/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

Condition keys	Description	Type
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/RoutingMode	Filters access by routing mode of the domain name. Available during the CreateDomainName and UpdateDomainName operations	String
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

Condition keys	Description	Type
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/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

Condition keys	Description	Type
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/RoutingMode	Filters access by routing mode of the domain name. Available during the UpdateDomainName and DeleteDomainName operations	String
apigateway:Resource/SecurityPolicy	Filters access by TLS version. Available during UpdateDomain and DeleteDomain operations	ArrayOfString
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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePortal	Grants permission to create a Portal	Write	Portal*		
				apigateway:Request/PortalDisplayName apigateway:Request/PortalDomainName apigateway:Request/CognitoU	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				serPoolArn aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortalProduct	Grants permission to create a Portal Product	Write	PortalProduct*		
				apigateway:Request/PortalProductDisplayName aws:RequestTag/${TagKey} aws:TagKeys	
CreateProductPage	Grants permission to create a Product Page	Write	ProductPage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				apigateway:Request/ProductPageTitle	
CreateProductRestEndpointPage	Grants permission to create a Product REST Endpoint Page	Write	ProductRestEndpointPage*		
				apigateway:Request/RestApiId apigateway:Request/Stage apigateway:Request/Method apigateway:Request/ProductRestEndpointPageEndpointPrefix	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRoutingRule	Grants permission to create a routing rule	Write	RoutingRule*	apigateway:Request/Priority apigateway:Request/ConditionBasePaths	
				aws:ResourceTag/${TagKey} apigateway:Request/Priority apigateway:Request/ConditionBasePaths	
DELETE	Grants permission to delete a particular resource	Write	AccessLogSettings		
			Api		
			ApiMapping		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePortal	Grants permission to delete a Portal	Write	Portal*		
DeletePortalProduct	Grants permission to delete a Portal Product	Write	PortalProduct*		
DeletePortalProductSharingPolicy	Grants permission to delete a Portal Product Sharing Policy	Permissions management	PortalProduct*		
DeleteProductPage	Grants permission to delete a Product Page	Write	ProductPage*		
DeleteProductRestEndpointPage	Grants permission to delete a Product REST Endpoint Page	Write	PortalProduct* ProductRestEndpointPage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoutingRule	Grants permission to delete a routing rule	Write	RoutingRule*	apigateway:Resource/Priority apigateway:Resource/ConditionBasePaths	
				aws:ResourceTag/${TagKey} apigateway:Resource/Priority apigateway:Resource/ConditionBasePaths	
DisablePortal	Grants permission to disable a Portal	Write	Portal*		
GET	Grants permission to read a particular resource	Read	AccessLogSettings		
			Api		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ApiMapping		
			ApiMappings		
			Apis		
			Authorizer		
			Authorizers		
			AuthorizersCache		
			Cors		
			Deployment		
			Deployments		
			ExportedAPI		
			Integration		
			IntegrationResponse		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			IntegrationResponses		
			Integrations		
			Model		
			ModelTemplate		
			Models		
			Route		
			RouteRequestParameter		
			RouteResponse		
			RouteResponses		
			RouteSettings		
			Routes		
			Stage		
			Stages		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VpcLink		
			VpcLinks		
GetPortal	Grants permission to read a Portal	Read	Portal*		
GetPortalProduct	Grants permission to read a Portal Product	Read	PortalProduct*		
GetPortalProductSharingPolicy	Grants permission to read a Portal Product Sharing Policy	Read	PortalProduct*		
GetProductPage	Grants permission to read a Product Page	Read	ProductPage*		
			PortalProduct		
GetProductRestEndpointPage	Grants permission to read a Product REST Endpoint Page	Read	ProductRestEndpointPage*		
			PortalProduct		
GetRoutingRule	Grants permission to read a routing rule	Read	RoutingRule*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPortalProducts	Grants permission to list Portal Products	List	PortalProduct*		
ListPortals	Grants permission to list Portals	List	Portal*		
ListProductPages	Grants permission to list Product Pages	List	ProductPage*		
			PortalProduct		
ListProductRestEndpointPages	Grants permission to list Product REST Endpoint Pages	List	ProductRestEndpointPage*		
			PortalProduct		
ListRoutingRules	Grants permission to list routing rules under a domain name	List	RoutingRule*		
				aws:ResourceTag/${TagKey}	
PATCH	Grants permission to update a particular resource	Write	Api		
			ApiMapping		
			Authorizer		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Deployment		
			Integration		
			IntegrationResponse		
			Model		
			Route		
			RouteRequestParameter		
			RouteResponse		
			Stage		
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
POST	Grants permission to create a particular resource	Write	ApiMappings		
			Apis		
			Authorizers		
			Deployments		
			IntegrationResponses		
			Integrations		
			Models		
			RouteResponses		
			Routes		
			Stages		
			VpcLinks		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
PUT	Grants permission to update a particular resource	Write	Api		
			Apis		
				aws:RequestTag/${TagKey} aws:TagKeys	
PreviewPortal	Grants permission to preview a Portal	Write	Portal*		
PublishPortal	Grants permission to publish a Portal	Write	Portal*		
PutPortalProductSharingPolicy	Grants permission to put a Portal Product Sharing Policy	Permissions management	PortalProduct*		
UpdatePortal	Grants permission to update a Portal	Write	Portal*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				apigateway:Request/PortalDisplayName apigateway:Request/PortalDomainName apigateway:Request/CognitoUserPoolArn aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortalProduct	Grants permission to update a Portal Product	Write	PortalProduct*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				apigateway:Request/PortalProductDisplayName aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProductPage	Grants permission to update a Product Page	Write	ProductPage*		
				apigateway:Request/ProductPageTitle	
UpdateProductRestEndpointPage	Grants permission to update a Product REST Endpoint Page	Write	ProductRestEndpointPage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				apigateway:Request/ProductRestEndpointPageEndpointPrefix	
UpdateRoutingRule	Grants permission to update a routing rule using the PutRoutingRule API	Write	RoutingRule*	apigateway:Request/Priority apigateway:Request/ConditionBasePaths apigateway:Resource/Priority apigateway:Resource/ConditionBasePaths	

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

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
AccessLog Settings	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 apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/ApiName apigateway:Resource/AuthorizerType

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

Resource types	ARN	Condition keys
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}
RoutingRule	arn:${Partition}:apigateway:${Region}:${Account}:/domainnames/${DomainName}/routingrules/${RoutingRuleId}	apigateway:Resource/ConditionBasePaths apigateway:Resource/Priority aws:ResourceTag/${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}

Resource types	ARN	Condition keys
Stages	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat aws:ResourceTag/${TagKey}
VpcLink	arn:${Partition}:apigateway:${Region}::/vpclinks/${VpcLinkId}	aws:ResourceTag/${TagKey}
VpcLinks	arn:${Partition}:apigateway:${Region}::/vpclinks	aws:ResourceTag/${TagKey}
Portal	arn:${Partition}:apigateway:${Region}:${Account}:/portals/${PortalId}	apigateway:Resource/CognitoUserPoolArn apigateway:Resource/PortalDisplayName apigateway:Resource/PortalDomainName apigateway:Resource/PortalPublishStatus aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
PortalProduct	arn:${Partition}:apigateway:${Region}:${Account}:/portalproducts/${PortalProductId}	apigateway:Resource/PortalProductDisplayName aws:ResourceTag/${TagKey}
ProductPage	arn:${Partition}:apigateway:${Region}:${Account}:/portalproducts/${PortalProductId}/productpages/${ProductPageId}	apigateway:Resource/ProductPageTitle aws:ResourceTag/${TagKey}
ProductRestEndpointPage	arn:${Partition}:apigateway:${Region}:${Account}:/portalproducts/${PortalProductId}/productrestendpointpages/${ProductRestEndpointPageId}	apigateway:Resource/Method apigateway:Resource/ProductRestEndpointPageEndpointPrefix apigateway:Resource/RestApiId apigateway:Resource/Stage 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 AWS 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
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/CognitoUserPoolArn	Filters access by a Portal's CognitoUserPoolArn that is passed in the request	ARN

Condition keys	Description	Type
apigateway:Request/ConditionBasePaths	Filters access by base paths defined on the condition of a routing rule. Available during the CreateRoutingRule and UpdateRoutingRule operations	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/Method	Filters access by a ProductRestEndpointPage's HTTP Method that is passed in the request	String
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/PortalDisplayName	Filters access by a Portal's Display Name that is passed in the request	String

Condition keys	Description	Type
apigateway:Request/PortalDomainName	Filters access by a Portal's vanity domain name that is passed in the request	String
apigateway:Request/PortalProductDisplayName	Filters access by a PortalProduct's Display Name that is passed in the request	String
apigateway:Request/Priority	Filters access by priority of the routing rule. Available during the CreateRoutingRule and UpdateRoutingRule operations	Numeric
apigateway:Request/ProductPageTitle	Filters access by a ProductPage's Title that is passed in the request	String
apigateway:Request/ProductRestEndpointPageEndpointPrefix	Filters access by a ProductRestEndpointPage's EndpointPrefix that is passed in the request	String
apigateway:Request/RestApiId	Filters access by a ProductRestEndpointPage's Amazon API Gateway API ID that is passed in the request	String
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

Condition keys	Description	Type
apigatewa y:Request/ RoutingMode	Filters access by routing mode of the domain name. Available during the CreateDomainName and UpdateDomainName operations	String
apigatewa y:Request/ SecurityPolicy	Filters access by TLS version. Available during the CreateDomain and UpdateDomain operations	ArrayOfString
apigatewa y:Request/Stage	Filters access by a ProductRestEndpointPage's Amazon API Gateway Stage Name that is passed in the request	String
apigatewa y:Request/ StageName	Filters access by stage name of the deployment that you attempt to create. Available during the CreateDep loyment operation	String
apigatewa y:Resourc e/AccessL oggingDes tination	Filters access by access log destination of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
apigatewa y:Resourc e/AccessL oggingFormat	Filters access by access log format of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
apigatewa y:Resource/ ApiKeyRequired	Filters access by the requirement of API key for the existing Route resource. Available during the UpdateRou te and DeleteRoute operations. Also available as a collection during reimport	ArrayOfBool
apigatewa y: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/CognitoUserPoolArn	Filters access by a Portal's CognitoUserPoolArn associated with the resource	ARN
apigateway:Resource/ConditionBasePaths	Filters access by base paths defined on the condition of the existing routing rule. Available during the UpdateRoutingRule and DeleteRoutingRule operations	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/Method	Filters access by a ProductRestEndpointPage's HTTP Method associated with the resource	String

Condition keys	Description	Type
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/PortalDisplayName	Filters access by a Portal's Display Name associated with the resource	String
apigateway:Resource/PortalDomainName	Filters access by a Portal's vanity domain name associated with the resource	String
apigateway:Resource/PortalProductDisplayName	Filters access by a PortalProduct's Display Name associated with the resource	String
apigateway:Resource/PortalPublishStatus	Filters access by a Portal's published status associated with the resource	String
apigateway:Resource/Priority	Filters access by priority of the existing routing rule. Available during the UpdateRoutingRule and DeleteRoutingRule operations	Numeric

Condition keys	Description	Type
apigateway:Resource/ProductPageTitle	Filters access by a ProductPage's Title associated with the resource	String
apigateway:Resource/ProductRestEndpointPageEndpointPrefix	Filters access by a ProductRestEndpointPage's EndpointPrefix associated with the resource	String
apigateway:Resource/RestApiId	Filters access by a ProductRestEndpointPage's Amazon API Gateway API ID associated with the resource	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
apigateway:Resource/RoutingMode	Filters access by routing mode of the existing domain name. Available during the UpdateDomainName and DeleteDomainName operations	String
apigateway:Resource/SecurityPolicy	Filters access by TLS version. Available during the UpdateDomainName and DeleteDomainName operations	ArrayOfString
apigateway:Resource/Stage	Filters access by a ProductRestEndpointPage's Amazon API Gateway Stage Name associated with the resource	String
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

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

Actions, resources, and condition keys for AWS App Mesh

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGatewayRoute	Grants permission to create a gateway route that is	Write	gatewayRoute*	aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	associated with a virtual gateway			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		
CreateVirtualGateway	Grants permission to create a virtual gateway within a service mesh	Write	virtualGateway*		

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

AWS 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 AWS 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 AWS App Mesh Preview

AWS App Mesh Preview (service prefix: `appmesh-preview`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

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

Topics

Actions defined by AWS App Mesh Preview

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGatewayRoute	Grants permission to create a gateway route that is associated with a virtual gateway	Write	gatewayRoute*		
			virtualService		
CreateMesh	Grants permission to create a service mesh	Write	mesh*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRoute	Grants permission to create a route that is associated with a virtual router	Write	route*		
			virtualNode		
CreateVirtualGateway	Grants permission to create a virtual gateway within a service mesh	Write	virtualGateway*		
CreateVirtualNode	Grants permission to create a virtual node within a service mesh	Write	virtualNode*		
			virtualService		
CreateVirtualRouter	Grants permission to create a virtual router within a service mesh	Write	virtualRouter*		
CreateVirtualService	Grants permission to create a virtual service within a service mesh	Write	virtualService*		
			virtualNode		
			virtualRouter		
DeleteGatewayRoute	Grants permission to delete an existing gateway route	Write	gatewayRoute*		
DeleteMesh	Grants permission to delete an existing service mesh	Write	mesh*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
ListVirtualGateways	Grants permission to list existing virtual gateways in a service mesh	List	mesh*		
ListVirtualNodes	Grants permission to list existing virtual nodes	List	mesh*		
ListVirtualRouters	Grants permission to list existing virtual routers in a service mesh	List	mesh*		

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

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

Resource types defined by AWS App Mesh Preview

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:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}`	

Resource types	ARN	Condition keys
virtualService	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}	
virtualNode	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}	
virtualRouter	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}	
route	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}/route/${RouteName}	
virtualGateway	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	
gatewayRoute	arn:${Partition}:appmesh-preview:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	

Condition keys for AWS App Mesh Preview

App Mesh Preview has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS App Runner

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

References:

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

Topics

Actions defined by AWS App Runner

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateCustomDomain	Grants permission to associate your own domain name with the AWS App Runner subdomain URL of your App Runner service	Write	service*		
AssociateWebAcl [permission only]	Grants permission to associate the service with an AWS WAF web ACL	Write	service* webacl*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutoScalingConfiguration	Grants permission to create an AWS App Runner automatic scaling configuration resource	Write	autoscalingconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Grants permission to create an AWS App Runner connection resource	Write	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateObservabilityConfiguration	Grants permission to create an AWS App Runner observability configuration resource	Write	observabilityconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateService	Grants permission to create an AWS App Runner service resource	Write	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
CreateVpcConnector	Grants permission to create an AWS App Runner VPC connector resource	Write	vpcconnector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcIngressConnection	Grants permission to create an AWS App Runner VpcIngressConnection resource	Write	vpcingressconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys apprunner:ServiceArn apprunner:VpcId apprunner:VpcEndpointId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAutoScalingConfiguration	Grants permission to delete an AWS App Runner automatic scaling configuration resource	Write	autoscalingconfiguration*		
DeleteConnection	Grants permission to delete an AWS App Runner connection resource	Write	connection*		
DeleteObservabilityConfiguration	Grants permission to delete an AWS App Runner observability configuration resource	Write	observabilityconfiguration*		
DeleteService	Grants permission to delete an AWS App Runner service resource	Write	service*		
DeleteVpcConnector	Grants permission to delete an AWS App Runner VPC connector resource	Write	vpcconnector*		
DeleteVpcIngressConnection	Grants permission to delete an AWS App Runner VpcIngressConnection resource	Write	vpcingressconnection*		
DescribeAutoScalingConfiguration	Grants permission to retrieve the description of an AWS App Runner automatic scaling configuration resource	Read	autoscalingconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCustomDomains	Grants permission to retrieve descriptions of custom domain names associated with an AWS App Runner service	Read	service*		
DescribeObservabilityConfiguration	Grants permission to retrieve the description of an AWS App Runner observability configuration resource	Read	observabilityconfiguration*		
DescribeOperation	Grants permission to retrieve the description of an operation that occurred on an AWS App Runner service	Read	service*		
DescribeService	Grants permission to retrieve the description of an AWS App Runner service resource	Read	service*		
DescribeVpcConnector	Grants permission to retrieve the description of an AWS App Runner VPC connector resource	Read	vpcconnector*		
DescribeVpcIngressConnection	Grants permission to retrieve the description of an AWS App Runner VpcIngressConnection resource	Read	vpcingressconnection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWebAclForService [permission only]	Grants permission to get the AWS WAF web ACL that is associated with an AWS App Runner service	Read	service*		
DisassociateCustomDomain	Grants permission to disassociate a custom domain name from an AWS App Runner service	Write	service*		
DisassociateWebAcl [permission only]	Grants permission to disassociate the service with an AWS WAF web ACL	Write	service*		
ListAssociatedServicesForWebAcl [permission only]	Grants permission to list the services that are associated with an AWS WAF web ACL	List	webacl*		
ListAutoScalingConfigurations	Grants permission to retrieve a list of AWS App Runner automatic scaling configurations in your AWS account	List			
ListConnections	Grants permission to retrieve a list of AWS App Runner connections in your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListObservabilityConfigurations	Grants permission to retrieve a list of AWS App Runner observability configurations in your AWS account	List			
ListOperations	Grants permission to retrieve a list of operations that occurred on an AWS App Runner service resource	List	service*		
ListServices	Grants permission to retrieve a list of running AWS App Runner services in your AWS account	List			
ListServicesForAutoScalingConfiguration	Grants permission to retrieve a list of associated AppRunner services of an AWS App Runner automatic scaling configuration in your AWS account	List	autoscalingconfiguration*		
ListTagsForResource	Grants permission to list tags associated with an AWS App Runner resource	Read	autoscalingconfiguration		
			connection		
			observabilityconfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service		
			vpcconnector		
ListVpcConnectors	Grants permission to retrieve a list of AWS App Runner VPC connectors in your AWS account	List			
ListVpcIngressConnections	Grants permission to retrieve a list of AWS App Runner VpcIngressConnections in your AWS account	List			
PauseService	Grants permission to pause an active AWS App Runner service	Write	service*		
ResumeService	Grants permission to resume an active AWS App Runner service	Write	service*		
StartDeployment	Grants permission to initiate a manual deployemnt to an AWS App Runner service	Write	service*		
TagResource	Grants permission to add tags to, or update tag values of, an AWS App Runner resource	Tagging	autoscalingconfiguration		
			connection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			observabilityconfiguration		
			service		
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from an AWS App Runner resource	Tagging	autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpcconnector		
			vpcingressconnection		
				aws:TagKeys	
UpdateDefaultAutoScalingConfiguration	Grants permission to update an AWS App Runner automatic scaling configuration to be the default in your AWS account	Write	autoscalingconfiguration*		
UpdateService	Grants permission to update an AWS App Runner service resource	Write	service*		
			autoscalingconfiguration		
			connection		
			observabilityconfiguration		
			vpcconnector		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				apprunner:ConnectionArn apprunner:AutoScalingConfigurationArn apprunner:ObservabilityConfigurationArn apprunner:VpcConnectorArn	
UpdateVpcIngressConnection	Grants permission to update an AWS App Runner VpcIngressConnection resource	Write	vpcingressconnection*		
				apprunner:VpcId apprunner:VpcEndpointId	

Resource types defined by AWS App Runner

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
service	`arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}`	aws:ResourceTag/${TagKey}
connection	`arn:${Partition}:apprunner:${Region}:${Account}:connection/${ConnectionName}/${ConnectionId}`	aws:ResourceTag/${TagKey}
autoscalingconfiguration	`arn:${Partition}:apprunner:${Region}:${Account}:autoscalingconfiguration/${AutoscalingConfigurationName}/${AutoscalingConfigurationVersion}/${AutoscalingConfigurationId}`	aws:ResourceTag/${TagKey}
observabilityconfiguration	`arn:${Partition}:apprunner:${Region}:${Account}:observabilityconfiguration/${ObservabilityConfigurationName}/${ObservabilityConfigurationVersion}/${ObservabilityConfigurationId}`	aws:ResourceTag/${TagKey}
vpcconnector	`arn:${Partition}:apprunner:${Region}:${Account}:vpcconnector/${VpcConnectorName}/${VpcConnectorVersion}/${VpcConnectorId}`	aws:ResourceTag/${TagKey}
vpcingressconnection	`arn:${Partition}:apprunner:${Region}:${Account}:vpcingressconnection/${V`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
	pcIngressConnectionName}/${VpcIngressConnectionId}	
webacl	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}	

Condition keys for AWS App Runner

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

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

Condition keys	Description	Type
apprunner:AutoScalingConfigurationArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated AutoScalingConfiguration resource	ARN
apprunner:ConnectionArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated Connection resource	ARN
apprunner:ObservabilityConfigurationArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated ObservabilityConfiguration resource	ARN
apprunner:ServiceArn	Filters access by the CreateVpcIngressConnection action based on the ARN of an associated Service resource	ARN

Condition keys	Description	Type
apprunner:VpcConnectorArn	Filters access by the CreateService and UpdateService actions based on the ARN of an associated VpcConnector resource	ARN
apprunner:VpcEndpointId	Filters access by the CreateVpcIngressConnection and UpdateVpcIngressConnection actions based on the VPC Endpoint in the request	String
apprunner:VpcId	Filters access by the CreateVpcIngressConnection and UpdateVpcIngressConnection actions based on the VPC in the request	String
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 AWS App Studio

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

References:

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

Topics

- Actions defined by AWS App Studio

- Resource types defined by AWS App Studio
- Condition keys for AWS App Studio

Actions defined by AWS App Studio

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountStatus [permission only]	Grants permission to describe the account's current status	Read			
GetEnablementJobStatus [permission only]	Grants permission to fetch status of a enablement job	Read			
StartEnablementJob [permission only]	Grants permission to submit a enablement job	Write			
StartRollbackEnablementJob [permission only]	Grants permission to rollback an enablement job	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTeam Deployment [permission only]	Grants permission to start a team deployment	Write			

Resource types defined by AWS App Studio

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:${Partition}:appstudio:${Region}:${Account}:instance/${InstanceId}`	
application	`arn:${Partition}:appstudio:${Region}:${Account}:application/${ApplicationId}`	
connector	`arn:${Partition}:appstudio:${Region}:${Account}:connector/${ConnectionId}`	

Condition keys for AWS App Studio

App Studio has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS App2Container

AWS App2Container (service prefix: `a2c`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

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

Topics

Actions defined by AWS App2Container

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContainerizationJobDetails	Grants permission to get the details of all Containerization jobs	Read			
GetDeploymentJobDetails	Grants permission to get the details of all Deployment jobs	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartContainerizationJob	Grants permission to start a Containerization job	Write			
StartDeploymentJob	Grants permission to start a Deploymnet job	Write			

Resource types defined by AWS App2Container

AWS App2Container does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS App2Container, specify `"Resource": "*"` in your policy.

Condition keys for AWS App2Container

App2Container has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS AppConfig

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

References:

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

Topics

- Actions defined by AWS AppConfig

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

Actions defined by AWS AppConfig

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

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

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

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

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

Note

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
DeleteExtension	Grants permission to delete an extension	Write	extension*		
DeleteExtensionAssociation	Grants permission to delete an extension association	Write	extensionassociation*		

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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/${TagKey}	
GetExtensionAssociation	Grants permission to view details about an extension association	Read	extensionassociation*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ListDeploymentStrategies	Grants permission to list the deployment strategies for your account	List			
ListDeployments	Grants permission to list the deployments for an environment	List	application*		

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

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

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

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

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

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

Resource types defined by AWS AppConfig

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

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

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

Condition keys for AWS AppConfig

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

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

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

Actions, resources, and condition keys for AWS AppFabric

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

References:

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

Topics

Actions defined by AWS AppFabric

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetUserAccessTasks	Grants permission to start user access tasks for multiple users	Write	appbundle*		
ConnectAppAuthorization	Grants permission to connect app authorizations	Write	appauthorization*		
			appbundle*		
CreateAppAuthorization	Grants permission to create app authorizations for app bundles	Write	appbundle*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBundle	Grants permission to create app bundles in your account	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestion	Grants permission to create ingestions for app bundles	Write	appbundle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngestionDestination	Grants permission to create ingestion destinations for app bundles	Write	appbundle*		
			ingestion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppAuthorization	Grants permission to delete app authorizations within an app bundle	Write	appauthorization* appbundle*		
DeleteAppBundle	Grants permission to delete app bundles in your account	Write	appbundle*		
DeleteIngestion	Grants permission to delete ingestions within an app bundle	Write	appbundle* ingestion*		
DeleteIngestionDestination	Grants permission to delete destinations within an ingestion	Write	appbundle* ingestion* ingestiondestination*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAppAuthorization	Grants permission to view details about app authorizations	Read	appauthorization*		
			appbundle*		
				aws:ResourceTag/${TagKey}	
GetAppBundle	Grants permission to view details about app bundles	Read	appbundle*		
				aws:ResourceTag/${TagKey}	
GetIngestion	Grants permission to view details about ingestions	Read	appbundle*		
			ingestion*		
				aws:ResourceTag/${TagKey}	
GetIngestionDestination	Grants permission to view details about ingestion destinations	Read	appbundle*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	
ListAppAuthorizations	Grants permission to retrieve a list of app authorizations within an app bundle	List	appbundle*		
ListAppBundles	Grants permission to retrieve a list of app bundles in your account	List			
ListIngestionDestinations	Grants permission to retrieve a list of destinations within an ingestion	List	appbundle*		
			ingestion*		
ListIngestions	Grants permission to retrieve a list of ingestions within an app bundle	List	appbundle*		
ListTagsForResource	Grants permission to list tags for AppFabric resources	Read	appauthorization		
			appbundle		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ingestion		
			ingestiondestination		
StartIngestion	Grants permission to start ingestions	Write	appbundle*		
			ingestion*		
StartUserAccessTasks	Grants permission to start user access tasks	Write	appbundle*		
StopIngestion	Grants permission to stop ingestions	Write	appbundle*		
			ingestion*		
TagResource	Grants permission to tag AppFabric resources	Tagging	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag AppFabric resources	Tagging	appauthorization		
			appbundle		
			ingestion		
			ingestiondestination		
				aws:TagKeys	
UpdateAppAuthorization	Grants permission to update app authorizations within app bundles	Write	appauthorization*		
			appbundle*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateIngestionDestination	Grants permission to update destinations within ingestions	Write	appbundle*		
			ingestion*		
			ingestiondestination*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS AppFabric

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
appbundle	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppBundleIdentifier}	aws:ResourceTag/${TagKey}
appauthorization	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/appauthorization/${AppAuthorizationIdentifier}	aws:ResourceTag/${TagKey}
ingestion	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}	aws:ResourceTag/${TagKey}
ingestion destination	arn:${Partition}:appfabric:${Region}:${Account}:appbundle/${AppbundleId}/ingestion/${IngestionIdentifier}/ingestiondestination/${IngestionDestinationIdentifier}	aws:ResourceTag/${TagKey}

Condition keys for AWS AppFabric

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

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

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

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

Actions, resources, and condition keys for Amazon AppFlow

Amazon AppFlow (service prefix: `appflow`) 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 AppFlow
- Resource types defined by Amazon AppFlow
- Condition keys for Amazon AppFlow

Actions defined by Amazon AppFlow

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelFlowExecutions	Grants permission to cancel in-progress executions of an Amazon AppFlow flow	Write	flow*		
CreateConnectorProfile	Grants permission to create a login profile to be used with Amazon AppFlow flows	Write			
CreateFlow	Grants permission to create an Amazon AppFlow flow	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnectorProfile	Grants permission to delete a login profile configured in Amazon AppFlow	Write	connectorprofile*		
DeleteFlow	Grants permission to delete an Amazon AppFlow flow	Write	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeConnector	Grants permission to describe a connector registered in Amazon AppFlow	Read	connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConnectorEntity	Grants permission to describe all fields for an object in a login profile configured in Amazon AppFlow	Read	connectorprofile*		
DescribeConnectorFields [permission only]	Grants permission to describe all fields for an object in a login profile configured in Amazon AppFlow (Console Only)	Read	connectorprofile*		
DescribeConnectorProfiles	Grants permission to describe all login profiles configured in Amazon AppFlow	Read			
DescribeConnectors	Grants permission to describe all connectors supported by Amazon AppFlow	Read			
DescribeFlow	Grants permission to describe a specific flow configured in Amazon AppFlow	Read	flow*		
DescribeFlowExecution [permission only]	Grants permission to describe all flow executions for a flow configured in Amazon AppFlow (Console Only)	Read	flow*		
DescribeFlowExecutionRecords	Grants permission to describe all flow executions for a flow configured in Amazon AppFlow	Read	flow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFlows [permission only]	Grants permission to describe all flows configured in Amazon AppFlow (Console Only)	Read			
ListConnectorEntities	Grants permission to list all objects for a login profile configured in Amazon AppFlow	List	connectorprofile*		
ListConnectorFields [permission only]	Grants permission to list all objects for a login profile configured in Amazon AppFlow (Console Only)	Read	connectorprofile*		
ListConnectors	Grants permission to list all connectors supported in Amazon AppFlow	List	connector*		
ListFlows	Grants permission to list all flows configured in Amazon AppFlow	List	flow*		
ListTagsForResource	Grants permission to list tags for a flow	Read	flow*		
RegisterConnector	Grants permission to register an Amazon AppFlow connector	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetConnectorMetadataCache	Grants permission to resets metadata of connector entities that Amazon AppFlow stored in its cache	Write	connectorprofile*		
RunFlow [permission only]	Grants permission to run a flow configured in Amazon AppFlow (Console Only)	Write	flow*		
StartFlow	Grants permission to activate (for scheduled and event-triggered flows) or run (for on-demand flows) a flow configured in Amazon AppFlow	Write	flow*		
StopFlow	Grants permission to deactivate a scheduled or event-triggered flow configured in Amazon AppFlow	Write	flow*		
TagResource	Grants permission to tag a flow or a connector	Tagging	connector		
			flow		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnRegisterConnector	Grants permission to un-register a connector in Amazon AppFlow	Write	connector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a flow or a connector	Tagging	connector		
			flow		
				aws:TagKeys	
UpdateConnectorProfile	Grants permission to update a login profile configured in Amazon AppFlow	Write	connectorprofile*		
UpdateConnectorRegistration	Grants permission to update a registered connector configured in Amazon AppFlow	Write	connector*		
UpdateFlow	Grants permission to update a flow configured in Amazon AppFlow	Write	flow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UseConnectorProfile [permission only]	Grants permission to use a connector profile while creating a flow in Amazon AppFlow	Write	connector profile*		

Resource types defined by Amazon AppFlow

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
connector profile	`arn:${Partition}:appflow:${Region}:${Account}:connectorprofile/${ProfileName}`	
flow	`arn:${Partition}:appflow:${Region}:${Account}:flow/${FlowName}`	aws:ResourceTag/${TagKey}
connector	`arn:${Partition}:appflow:${Region}:${Account}:connector/${ConnectorLabel}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon AppFlow

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

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

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by allowed set of values for each of the tags	String
aws:ResourceTag/${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 AppIntegrations

Amazon AppIntegrations (service prefix: `app-integrations`) 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 AppIntegrations
- Resource types defined by Amazon AppIntegrations
- Condition keys for Amazon AppIntegrations

Actions defined by Amazon AppIntegrations

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create a new Application	Write	application*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssociation [permission only]	Grants permission to create an ApplicationAssociation	Write	application*		
				aws:RequestTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataIntegration	Grants permission to create a new DataIntegration	Write	data-integration*		appflow:DeleteFlow appflow:DescribeConnectorProfiles iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant profile:GetDomain profile:GetProfileObjectType s3:GetBucketNotification

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetEncryptionConfiguration s3:PutBucketNotification
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataIntegrationAssociation	Grants permission to create a DataIntegrationAssociation	Write	data-integration*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:TagResource appflow:UseConnectorProfile profile:CreateSnapshot profile:GetSnapshot

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataIntegrationSchedule	Grants permission to create a data integration schedule	Write	data-integration*		
CreateEventIntegration	Grants permission to create a new EventIntegration	Write	event-integration*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventIntegrationAssociation [permission only]	Grants permission to create an EventIntegrationAssociation	Write	event-integration*		events:PutRule events:PutTargets
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Grants permission to delete an Application	Write	application*		
				aws:ResourceTag/${TagKey}	
DeleteApplicationAssociation [permission only]	Grants permission to delete an ApplicationAssociation	Write	application-association*		
DeleteDataIntegration	Grants permission to delete a DataIntegration	Write	data-integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteDataIntegrationAssociation [permission only]	Grants permission to delete a DataIntegrationAssociation	Write	data-integration-association*		appflow:CreateFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:DescribeConnectorProfiles appflow:StopFlow appflow:TagResource appflow:UseConnectorProfile
DeleteEventIntegration	Grants permission to delete an EventIntegration	Write	event-integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteEventIntegrationAssociation [permission only]	Grants permission to delete an EventIntegrationAssociation	Write	event-integration-association*		events:DeleteRule events:ListTargetsByRule events:RemoveTargets
GetApplication	Grants permission to view details about Application	Read	application*		
				aws:ResourceTag/${TagKey}	
GetDataIntegration	Grants permission to view details about DataIntegrations	Read	data-integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataIntegrationExecution	Grants permission to get details about a data integration execution	Read	data-integration*		
GetDataIntegrationSchedule	Grants permission to get details about a data integration schedule	Read	data-integration*		
GetEventIntegration	Grants permission to view details about EventIntegrations	Read	event-integration*		
				aws:ResourceTag/${TagKey}	
ListApplicationAssociations	Grants permission to list ApplicationAssociations	List			
ListApplications	Grants permission to list Applications	List			
ListDataIntegrationAssociations	Grants permission to list DataIntegrationAssociations	List			
ListDataIntegrationExecutions	Grants permission to list data integration executions	List	data-integration*		
ListDataIntegrationSchedules	Grants permission to list data integration schedules	List	data-integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataIntegrations	Grants permission to list DataIntegrations	List			
ListEventIntegrationAssociations	Grants permission to list EventIntegrationAssociations	Read			
ListEventIntegrations	Grants permission to list EventIntegrations	List			
ListTagsForResource	Grants permission to lists tag for an Amazon AppIntegration resource	Read	application		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDataIntegrationExecution	Grants permission to start a data integration execution	Write	data-integration*		profile:CreateSegmentSnapshot profile:CreateSnapshot
TagResource	Grants permission to tag an Amazon AppIntegration resource	Tagging	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		
			event-integration-association		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an Amazon AppIntegration resource	Tagging	application		
			application-association		
			data-integration		
			data-integration-association		
			event-integration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			event-integration-association		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApplication	Grants permission to modify an Application	Write	application*		
				aws:ResourceTag/${TagKey}	
UpdateDataIntegration	Grants permission to modify a DataIntegration	Write	data-integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataIntegrationAssociation	Grants permission to modify a DataIntegrationAssociation	Write	data-integration-association*		profile:CreateSnapshot profile:GetSnapshot
				aws:ResourceTag/${TagKey}	
UpdateDataIntegrationSchedule	Grants permission to update a data integration schedule	Write	data-integration*		
UpdateEventIntegration	Grants permission to modify an EventIntegration	Write	event-integration*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon AppIntegrations

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-integration	arn:${Partition}:app-integrations:${Region}:${Account}:event-integration/${EventIntegrationName}	aws:ResourceTag/${TagKey}
event-integration-association	arn:${Partition}:app-integrations:${Region}:${Account}:event-integration-association/${EventIntegrationName}/${ResourceId}	aws:ResourceTag/${TagKey}
data-integration	arn:${Partition}:app-integrations:${Region}:${Account}:data-integration/${DataIntegrationId}	aws:ResourceTag/${TagKey}
data-integration-association	arn:${Partition}:app-integrations:${Region}:${Account}:data-integration-association/${DataIntegrationId}/${ResourceId}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:app-integrations:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
application-association	arn:${Partition}:app-integrations:${Region}:${Account}:application-association/${ApplicationId}/${ApplicationAssociationId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon AppIntegrations

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

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

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

Actions, resources, and condition keys for AWS Application Auto Scaling

AWS 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 AWS Application Auto Scaling
- Resource types defined by AWS Application Auto Scaling
- Condition keys for AWS Application Auto Scaling

Actions defined by AWS 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 AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aling:scalable-dimension	
DeregisterScalableTarget	Grants permission to deregister a scalable target	Write	ScalableTarget*		
				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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScalingPolicies	Grants permission to describe a set of scaling policies or all scaling policies in the specified namespace	Read			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
PutScheduledAction	Grants permission to create and update a scheduled action for a scalable target	Write	ScalableTarget*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
RegisterScalableTarget	Grants permission to register AWS 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 AWS 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 AWS Application Auto Scaling

AWS 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 AWS 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 Application Discovery Arsenal

Application Discovery Arsenal (service prefix: `arsenal`) 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 Application Discovery Arsenal

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterOnPremisesAgent [permission only]	Grants permission to register AWS provided data collectors to the Application Discovery Service	Write			

Resource types defined by Application Discovery Arsenal

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

Condition keys for Application Discovery Arsenal

Application Discovery Arsenal has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Application Discovery Service

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

References:

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

Topics

Actions defined by AWS Application Discovery Service

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateConfigurationItemsToApplication	Grants permission to AssociateConfigurationItemsToApplication API. AssociateConfigurationItemsToApplication associates one or more configuration items with an application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteAgents	Grants permission to BatchDeleteAgents API. BatchDeleteAgents deletes one or more agents/data collectors associated with your account, each identified by its agent ID. Deleting a data collector does not delete the previous data collected	Write			
BatchDeleteImportData	Grants permission to BatchDeleteImportData API. BatchDeleteImportData deletes one or more Migration Hub import tasks, each identified by their import ID. Each import task has a number of records, which can identify servers or applications	Write			
CreateApplication	Grants permission to CreateApplication API. CreateApplication creates an application with the given name and description	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTags	Grants permission to CreateTags API. CreateTags creates one or more tags for configuration items. Tags are metadata that help you categorize IT assets. This API accepts a list of multiple configuration items	Tagging			
DeleteApplications	Grants permission to DeleteApplications API. DeleteApplications deletes a list of applications and their associations with configuration items	Write			
DeleteTags	Grants permission to DeleteTags API. DeleteTags deletes the association between configuration items and one or more tags. This API accepts a list of multiple configuration items	Tagging		aws:TagKeys	
DescribeAgents	Grants permission to DescribeAgents API. DescribeAgents lists agents or the Connector by ID or lists all agents/Connectors associated with your user if you did not specify an ID	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBatchDeleteConfigurationTask	Grants permission to DescribeBatchDeleteConfigurationTask API. DescribeBatchDeleteConfigurationTask returns attributes about a batched deletion task to delete a set of configuration items. The supplied task ID should be the task ID receieved from the output of StartBatchDeleteConfigurationTask	Read			
DescribeConfigurations	Grants permission to DescribeConfigurations API. DescribeConfigurations retrieves attributes for a list of configuration item IDs. All of the supplied IDs must be for the same asset type (server, application, process, or connection). Output fields are specific to the asset type selected. For example, the output for a server configuration item includes a list of attributes about the server, such as host name, operating system, and number of network cards	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeContinuousExports	Grants permission to DescribeContinuousExports API. DescribeContinuous Exports lists exports as specified by ID. All continuous exports associated with your user can be listed if you call DescribeContinuousExports as is without passing any parameters	Read			
DescribeExportConfigurations	Grants permission to DescribeExportConfigurations API. DescribeExportConfigurations retrieves the status of a given export process. You can retrieve status from a maximum of 100 processes	Read			
DescribeExportTasks	Grants permission to DescribeExportTasks API. DescribeExportTasks retrieve status of one or more export tasks. You can retrieve the status of up to 100 export tasks	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImportTasks	Grants permission to DescribeImportTasks API. DescribeImportTasks returns an array of import tasks for your user, including status information, times, IDs, the Amazon S3 Object URL for the import file, and more	List			
DescribeTags	Grants permission to DescribeTags API. DescribeTags retrieves a list of configuration items that are tagged with a specific tag. Or retrieves a list of all tags assigned to a specific configuration item	Read			
DisassociateConfigurationItemsFromApplication	Grants permission to DisassociateConfigurationItemsFromApplication API. DisassociateConfigurationItemsFromApplication disassociates one or more configuration items from an application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportConfigurations	Grants permission to ExportConfigurations API. ExportConfigurations exports all discovered configuration data to an Amazon S3 bucket or an application that enables you to view and evaluate the data. Data includes tags and tag associations, processes , connections, servers, and system performance	Write			
GetDiscoverySummary	Grants permission to GetDiscoverySummary API. GetDiscoverySummary retrieves a short summary of discovered assets	Read			
GetNetworkConnectionGraph	Grants permission to GetNetworkConnectionGraph API. GetNetworkConnectionGraph accepts input list of one of - Ip Addresses, server ids or node ids. Returns a list of nodes and edges which help customer visualize network connection graph. This API is used for visualize network graph functionality in MigrationHub console	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfigurations	Grants permission to ListConfigurations API. ListConfigurations retrieves a list of configuration items according to criteria you specify in a filter. The filter criteria identify relationship requirements	List			
ListServerNeighbors	Grants permission to ListServerNeighbors API. ListServerNeighbors retrieves a list of servers which are one network hop away from a specified server	List			
StartBatchDeleteConfigurationTask	Grants permission to StartBatchDeleteConfigurationTask API. StartBatchDeleteConfigurationTask starts an asynchronous batch deletion of your configuration items. All of the supplied IDs must be for the same asset type (server, application, process, or connection). Output is a unique task ID you can use to check back on the deletions progress	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartContinuousExport	Grants permission to StartContinuousExport API. StartContinuousExport start the continuous flow of agent's discovered data into Amazon Athena	Write			iam:AttachRolePolicy iam:CreatePolicy iam:CreateRole iam:CreateServiceLinkedRole
StartDataCollectionByAgentIds	Grants permission to StartDataCollectionByAgentIds API. StartDataCollectionByAgentIds instructs the specified agents or Connectors to start collecting data	Write			
StartExportTask	Grants permission to StartExportTask API. StartExportTask export the configuration data about discovered configuration items and relationships to an S3 bucket in a specified format	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartImportTask	Grants permission to StartImportTask API. StartImportTask starts an import task. The Migration Hub import feature allows you to import details of your on-premises environment directly into AWS without having to use the Application Discovery Service (ADS) tools such as the Discovery Connector or Discovery Agent. This gives you the option to perform migration assessment and planning directly from your imported data including the ability to group your devices as applications and track their migration status	Write			discovery:AssociateConfigurationItemsToApplication discovery:CreateApplication discovery:CreateTags discovery:GetDiscoverySummary discovery:ListConfigurations s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopContinuousExport	Grants permission to StopContinuousExport API. StopContinuousExport stops the continuous flow of agent's discovered data into Amazon Athena	Write			
StopDataCollectionByAgentIds	Grants permission to StopDataCollectionByAgentIds API. StopDataCollectionByAgentIds instructs the specified agents or Connectors to stop collecting data	Write			
UpdateApplication	Grants permission to UpdateApplication API. UpdateApplication updates metadata about an application	Write			

Resource types defined by AWS Application Discovery Service

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

> **Note**
>
> To separate access, create and use separate AWS accounts.

Condition keys for AWS Application Discovery Service

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

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

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

Actions, resources, and condition keys for AWS Application Migration Service

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

References:

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

Topics

- Actions defined by AWS Application Migration Service
- Resource types defined by AWS Application Migration Service
- Condition keys for AWS Application Migration Service

Actions defined by AWS Application 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 AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ArchiveApplication	Grants permission to archive an application	Write	ApplicationResource*		
ArchiveWave	Grants permission to archive a wave	Write	WaveResource*		
AssociateApplications	Grants permission to associate applications to a wave	Write	ApplicationResource*		
			WaveResource*		
AssociateSourceServers	Grants permission to associate source servers to an application	Write	ApplicationResource*		
			SourceServerResource*		
BatchCreateVolumeSnapshotGroupForMgn [permission only]	Grants permission to create volume snapshot group	Write	SourceServerResource*		
BatchDeleteSnapshotRequestForMgn	Grants permission to batch delete snapshot request	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
ChangeServerLifeCycleState	Grants permission to change source server life cycle state	Write	SourceServerResource*		
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Grants permission to create connector	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfigurationTemplate	Grants permission to create launch configuration template	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkMigrationDefinition	Grants permission to create a network migration definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicationConfigurationTemplate	Grants permission to create replication configuration template	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVcenterClientForMgn [permission only]	Grants permission to create vcenter client	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWave	Grants permission to create a wave	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplication	Grants permission to delete an application	Write	ApplicationResource*		
DeleteConnector	Grants permission to delete connector	Write	ConnectorResource*		
DeleteJob	Grants permission to delete job	Write	JobResource*		
DeleteLaunchConfigurationTemplate	Grants permission to delete launch configuration template	Write	LaunchConfigurationTemplateResource*		
DeleteNetworkMigrationDefinition	Grants permission to delete a network migration definition	Write	NetworkMigrationDefinitionResource*		
DeleteReplicationConfigurationTemplate	Grants permission to delete replication configuration template	Write	ReplicationConfigurationTemplateResource*		
DeleteSourceServer	Grants permission to delete source server	Write	SourceServerResource*		
DeleteVcenterClient	Grants permission to delete vcenter client	Write	VcenterClientResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWave	Grants permission to delete a wave	Write	WaveResource*		
DescribeJobLogItems	Grants permission to describe job log items	Read	JobResource*		
DescribeJobs	Grants permission to describe jobs	List			
DescribeLaunchConfigurationTemplates	Grants permission to describe launch configuration template	List			
DescribeReplicationConfigurationTemplates	Grants permission to describe replication configuration template	List			
DescribeReplicationServerAssociationsForMgn [permission only]	Grants permission to describe replication server associations	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSnapshotRequestsForMgn [permission only]	Grants permission to describe snapshots requests	Read			
DescribeSourceServers	Grants permission to describe source servers	List			
DescribeVcenterClients	Grants permission to describe vcenter clients	List			
DisassociateApplications	Grants permission to disassociate applications from a wave	Write	ApplicationResource*		
			WaveResource*		
DisassociateSourceServers	Grants permission to disassociate source servers from an application	Write	ApplicationResource*		
			SourceServerResource*		
DisconnectFromService	Grants permission to disconnect source server from service	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
FinalizeCutover	Grants permission to finalize cutover	Write	SourceServerResource*		
GetAccountSettings	Grants permission to get account settings	Read			
GetAgentCommandForMgn [permission only]	Grants permission to get agent command	Read	SourceServerResource*		
GetAgentConfirmedResumeInfoForMgn [permission only]	Grants permission to get agent confirmed resume info	Read	SourceServerResource*		
GetAgentInstallationAssetsForMgn [permission only]	Grants permission to get agent installation assets	Read			
GetAgentReplicationInfoForMgn [permission only]	Grants permission to get agent replication info	Read	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAgentRuntimeConfigurationForMgn [permission only]	Grants permission to get agent runtime configuration	Read	SourceServerResource*		
GetAgentSnapshotCreditsForMgn [permission only]	Grants permission to get agent snapshots credits	Read	SourceServerResource*		
GetChannelCommandsForMgn [permission only]	Grants permission to get channel commands	Read			
GetLaunchConfiguration	Grants permission to get launch configuration	Read	SourceServerResource*		
GetNetworkMigrationDefinition	Grants permission to get a network migration definition	Read	NetworkMigrationDefinitionResource*		
GetNetworkMigrationMapperSegmentConstruct	Grants permission to get a network migration mapper segment construct	Read	NetworkMigrationDefinitionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReplicationConfiguration	Grants permission to get replication configuration	Read	SourceServerResource*		
GetVcenterClientCommandsForMgn [permission only]	Grants permission to get vcenter client commands	Read	VcenterClientResource*		
InitializeService	Grants permission to initialize service	Write			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile
IssueClientCertificateForMgn [permission only]	Grants permission to issue a client certificate	Write	SourceServerResource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Grants permission to list application summaries	List			
ListConnectors	Grants permission to list connectors	Read			
ListExportErrors	Grants permission to list the errors of an export task	List	ExportResource*		
ListExports	Grants permission to list export tasks	List			
ListImportErrors	Grants permission to list the errors of an import task	List	ImportResource*		
ListImportFileEnrichments	Grants permission to list the import file enrichment tasks	List			
ListImports	Grants permission to list the import tasks	List			
ListManagedAccounts	Grants permission to list managed accounts	List			
ListNetworkMigrationAnalyses	Grants permission to list network migration analyses	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationAnalysisResults	Grants permission to list network migration analysis results	List	NetworkMigrationDefinitionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNetworkMigrationCodeGenerationSegments	Grants permission to list network migration code generation segments	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationCodeGenerations	Grants permission to list network migration code generations	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDefinitions	Grants permission to list network migration definitions	List			
ListNetworkMigrationDeployedStacks	Grants permission to list network migration deployed stacks	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployedStacksDeletions	Grants permission to list network migration deployed stacks deletions	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationDeployments	Grants permission to list network migration deployments	List	NetworkMigrationDefinitionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNetworkMigrationExecutions	Grants permission to list network migration executions	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegmentConstructs	Grants permission to list network migration mapper segment constructs	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMapperSegments	Grants permission to list network migration mapper segments	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappingUpdates	Grants permission to list network migration mapping updates	List	NetworkMigrationDefinitionResource*		
ListNetworkMigrationMappings	Grants permission to list network migration mappings	List	NetworkMigrationDefinitionResource*		
ListSourceServerActions	Grants permission to list source server action documents	List	SourceServerResource*		
ListTagsForResource	Grants permission to list tags for a resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTemplateActions	Grants permission to list launch configuration template action documents	List	LaunchConfigurationTemplateResource*		
ListWaves	Grants permission to list wave summaries	List			
MarkAsArchived	Grants permission to mark source server as archived	Write	SourceServerResource*		
NotifyAgentAuthenticationForMgn [permission only]	Grants permission to notify agent authentication	Write	SourceServerResource*		
NotifyAgentConnectedForMgn [permission only]	Grants permission to notify agent is connected	Write	SourceServerResource*		
NotifyAgentDisconnectedForMgn [permission only]	Grants permission to notify agent is disconnected	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyAgentReplicationProgressForMgn [permission only]	Grants permission to notify agent replication progress	Write	SourceServerResource*		
NotifyVcenterClientStartedForMgn [permission only]	Grants permission to notify vcenter client started	Write	VcenterClientResource*		
PauseReplication	Grants permission to pause replication	Write	SourceServerResource*		
PutSourceServerAction	Grants permission to put source server action document	Write	SourceServerResource*		
PutTemplateAction	Grants permission to put launch configuration template action document	Write	LaunchConfigurationTemplateResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterAgentForMgn [permission only]	Grants permission to register agent	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveSourceServerAction	Grants permission to remove source server action document	Write	SourceServerResource*		
RemoveTemplateAction	Grants permission to remove launch configuration template action document	Write	LaunchConfigurationTemplateResource*		
ResumeReplication	Grants permission to resume replication	Write	SourceServerResource*		
RetryDataReplication	Grants permission to retry replication	Write	SourceServerResource*		
SendAgentLogsForMgn [permission only]	Grants permission to send agent logs	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendAgentMetricsForMgn [permission only]	Grants permission to send agent metrics	Write	SourceServerResource*		
SendChannelCommandResultForMgn [permission only]	Grants permission to send channel command result	Write			
SendClientLogsForMgn [permission only]	Grants permission to send client logs	Write			
SendClientMetricsForMgn [permission only]	Grants permission to send client metrics	Write			
SendVcenterClientCommandResultForMgn [permission only]	Grants permission to send vcenter client command result	Write	VcenterClientResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendVcenterClientLogsForMgn [permission only]	Grants permission to send vcenter client logs	Write	VcenterClientResource*		
SendVcenterClientMetricsForMgn [permission only]	Grants permission to send vcenter client metrics	Write	VcenterClientResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCutover	Grants permission to start cutover	Write	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartExport	Grants permission to start an export task	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeLaunchTemplateVersions mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves s3:PutObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartImport	Grants permission to create an import task	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:ModifyLaunchTemplate mgn:DescribeSourceServers mgn:GetLaunchConfiguration mgn:ListApplications mgn:ListWaves mgn:TagResource mgn:UpdateLaunchCo

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					nfiguration s3:PutObject
StartImportFileEnrichment	Grants permission to start import file enrichment	Write			ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkMigrationAnalysis	Grants permission to start a network migration analysis	Write	NetworkMigrationDefinitionResource*		directconnect:DescribeConnections directconnect:DescribeDirectConnectGatewayAssociations directconnect:DescribeDirectConnectGatewayAttachments directconnect:DescribeDirectConnectGateways directconnect:DescribeVirtualGateways directconnect:Desc

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ribeVirtualInterfaces ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DeleteTags ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeManagedPrefixLists

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayV

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					pcAttachments ec2:DescribeTransitGateways ec2:DescribeVpcEndpointServiceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTablePropagations ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis elasticloadbalancing:DescribeListeners elasticloadbalancing:DescribeLoadBalancerAttributes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					elasticloadbalancing:DescribeLoadBalancers elasticloadbalancing:DescribeRules elasticloadbalancing:DescribeTags elasticloadbalancing:DescribeTargetGroupAttributes elasticloadbalancing:DescribeTargetGroups elasticloadbalancing:Descri

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					beTargetHealth globalaccelerator:ListAccelerators globalaccelerator:ListCustomRoutingAccelerators globalaccelerator:ListCustomRoutingEndpointGroups globalaccelerator:ListCustomRoutingListeners globalaccelerator:ListCustomRoutingP

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ortMappings globalaccelerator:ListEndpointGroups globalaccelerator:ListListeners network-firewall:DescribeFirewall network-firewall:DescribeFirewallPolicy network-firewall:DescribeResourcePolicy network-firewall:DescribeRuleGroup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					network-firewall:ListFirewallPolicies network-firewall:ListFirewalls network-firewall:ListRuleGroups tiros:CreateQuery tiros:ExtendQuery tiros:GetQueryAnswer tiros:GetQueryExplanation tiros:GetQueryExtensionAccounts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkMigrationCodeGeneration	Grants permission to start network migration code generation	Write	NetworkMigrationDefinitionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkMigrationDeployedStacksDeletion	Grants permission to start deletion of network migration deployed stacks	Write	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DetachInternetGateway ec2:DetachVolume

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DisableTransitGatewayRouteTablePropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:ModifyInstanceAttribute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkMigrationDeployment	Grants permission to start a network migration deployment	Write	NetworkMigrationDefinitionResource*		ec2:AcceptTransitGatewayVpcAttachment ec2:AssociateNatGatewayAddress ec2:AssociateRouteTable ec2:AssociateSubnetCidrBlock ec2:AssociateTransitGatewayRouteTable ec2:AssociateVpcCidrBlock ec2:AttachInternetGateway

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNatGateway ec2:CreateNetworkAcl ec2:CreateNetworkAclEntry ec2:CreateNetworkInsightsPath ec2:CreateNetworkInterface

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:CreateRoute ec2:CreateRouteTable ec2:CreateSecurityGroup ec2:CreateSubnet ec2:CreateTags ec2:CreateTransitGatewayRoute ec2:CreateTransitGatewayRouteTable ec2:CreateTransitGatewayVpcAttachment

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteInternetGateway ec2:DeleteLaunchTemplate ec2:DeleteLaunchTemplateVersions ec2:DeleteNatGateway ec2:DeleteNetworkAcl ec2:DeleteNetworkAclEntry ec2:DeleteNetworkInsightsAnalysis ec2:DeleteNetworkInsightsPath

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteNetworkInterface ec2:DeleteRoute ec2:DeleteRouteTable ec2:DeleteSecurityGroup ec2:DeleteSnapshot ec2:DeleteSubnet ec2:DeleteTransitGateway ec2:DeleteTransitGatewayRoute ec2:DeleteTransitGatewayRouteTable

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteTransitGatewayVpcAttachment ec2:DeleteVolume ec2:DeleteVpc ec2:DescribeAccountAttributes ec2:DescribeAddresses ec2:DescribeAvailabilityZones ec2:DescribeCustomerGateways ec2:DescribeEgressOnlyInter

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					netGateways ec2:DescribeHosts ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeInternetGateways ec2:DescribeLaunch

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					TemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeManagedPrefixLists ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeNetworkInsightsAnalyses ec2:DescribeNetworkInsightsPaths ec2:DescribeNetworkInterfaces

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribePrefixLists ec2:DescribeRegions ec2:DescribeRouteTables ec2:DescribeSecurityGroupRules ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeTransitGatewayAttachments

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeTransitGatewayConnects ec2:DescribeTransitGatewayPeeringAttachments ec2:DescribeTransitGatewayRouteTables ec2:DescribeTransitGatewayVpcAttachments ec2:DescribeTransitGateways ec2:DescribeVolumes ec2:DescribeVpcEndpointServ

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iceConfigurations ec2:DescribeVpcEndpoints ec2:DescribeVpcPeeringConnections ec2:DescribeVpcs ec2:DescribeVpnConnections ec2:DescribeVpnGateways ec2:DetachInternetGateway ec2:DetachVolume ec2:DisableTransitGatewayRouteTableP

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ropagation ec2:DisassociateNatGatewayAddress ec2:DisassociateRouteTable ec2:DisassociateTransitGatewayRouteTable ec2:EnableTransitGatewayRouteTablePropagation ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:GetManagedPrefixListEntries ec2:GetTransitGatewayRouteTableAssociations ec2:GetTransitGatewayRouteTablePropagations ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ModifySubnetAttribute ec2:ModifyTransitGateway

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ModifyTransitGatewayVpcAttachment ec2:ModifyVolume ec2:ModifyVpcAttribute ec2:RejectTransitGatewayVpcAttachment ec2:ReleaseAddress ec2:ReplaceNetworkAclAssociation ec2:ReplaceNetworkAclEntry ec2:ReplaceRoute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ReplaceTransitGatewayRoute ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress ec2:SearchTransitGatewayRoutes ec2:StartNetworkInsightsAnalysis
StartNetworkMigrationMapping	Grants permission to start a network migration mapping	Write	NetworkMigrationDefinitionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkMigrationMappingUpdate	Grants permission to start a network migration mapping update	Write	NetworkMigrationDefinitionResource*		
StartReplication	Grants permission to start replication	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTest	Grants permission to start test	Write	SourceServerResource*		ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSecurityGroup ec2:CreateSnapshot ec2:CreateTags ec2:CreateVolume

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets ec2:DescribeVolumes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:ReportInstanceStatus ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					mgn:ListTagsForResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopReplication	Grants permission to stop replication	Write	SourceServerResource*		
TagResource	Grants permission to assign a resource tag	Tagging	ApplicationResource		
			ConnectorResource		
			ExportResource		
			ImportResource		
			JobResource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			LaunchConfigurationTemplateResource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:RequestTag/${TagKey} mgn:CreateAction aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TerminateTargetInstances	Grants permission to terminate target instances	Write	SourceServerResource*		ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveApplication	Grants permission to unarchive an application	Write	ApplicationResource*		
UnarchiveWave	Grants permission to unarchive a wave	Write	WaveResource*		
UntagResource	Grants permission to untag a resource	Tagging	ApplicationResource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Connector Resource		
			JobResource		
			LaunchConfigurationTemplate Resource		
			ReplicationConfigurationTemplateResource		
			SourceServerResource		
			VcenterClientResource		
			WaveResource		
				aws:TagKeys	
UpdateAccountSettings	Grants permission to update account settings	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgentBacklogForMgn [permission only]	Grants permission to update agent backlog	Write	SourceServerResource*		
UpdateAgentConversionInfoForMgn [permission only]	Grants permission to update agent conversion info	Write	SourceServerResource*		
UpdateAgentReplicationInfoForMgn [permission only]	Grants permission to update agent replication info	Write	SourceServerResource*		
UpdateAgentReplicationProcessStateForMgn [permission only]	Grants permission to update agent replication process state	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgentSourcePropertiesForMgn [permission only]	Grants permission to update agent source properties	Write	SourceServerResource*		
UpdateApplication	Grants permission to update an application	Write	ApplicationResource*		
UpdateConnector	Grants permission to update connector	Write	ConnectorResource*		
UpdateLaunchConfiguration	Grants permission to update launch configuration	Write	SourceServerResource*		
UpdateLaunchConfigurationTemplate	Grants permission to update launch configuration	Write	LaunchConfigurationTemplateResource*		
UpdateNetworkMigrationDefinition	Grants permission to update a network migration definition	Write	NetworkMigrationDefinitionResource*		
UpdateNetworkMigrationMapperSegment	Grants permission to update a network migration mapper segment	Write	NetworkMigrationDefinitionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNetworkMigrationMapperSegmentConstruct	Grants permission to update a network migration mapper segment construct	Write	NetworkMigrationDefinitionResource*		
UpdateReplicationConfiguration	Grants permission to update replication configuration	Write	SourceServerResource*		
UpdateReplicationConfigurationTemplate	Grants permission to update replication configuration template	Write	ReplicationConfigurationTemplateResource*		
UpdateSourceServer	Grants permission to update source server	Write	SourceServerResource*		
UpdateSourceServerReplicationType	Grants permission to update source server replication type	Write	SourceServerResource*		
UpdateWave	Grants permission to update a wave	Write	WaveResource*		
VerifyClientRoleForMgn [permission only]	Grants permission to verify client role	Read			

Resource types defined by AWS Application 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
JobResource	`arn:${Partition}:mgn:${Region}:${Account}:job/${JobID}`	aws:ResourceTag/${TagKey}
ReplicationConfigurationTemplateResource	`arn:${Partition}:mgn:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	`arn:${Partition}:mgn:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
VcenterClientResource	`arn:${Partition}:mgn:${Region}:${Account}:vcenter-client/${VcenterClientID}`	aws:ResourceTag/${TagKey}
SourceServerResource	`arn:${Partition}:mgn:${Region}:${Account}:source-server/${SourceServerID}`	aws:ResourceTag/${TagKey}
ApplicationResource	`arn:${Partition}:mgn:${Region}:${Account}:application/${ApplicationID}`	aws:ResourceTag/${TagKey}
WaveResource	`arn:${Partition}:mgn:${Region}:${Account}:wave/${WaveID}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ImportResource	arn:${Partition}:mgn:${Region}:${Account}:import/${ImportID}	aws:ResourceTag/${TagKey}
ExportResource	arn:${Partition}:mgn:${Region}:${Account}:export/${ExportID}	aws:ResourceTag/${TagKey}
ConnectorResource	arn:${Partition}:mgn:${Region}:${Account}:connector/${ConnectorID}	aws:ResourceTag/${TagKey}
NetworkMigrationDefinitionResource	arn:${Partition}:mgn:${Region}:${Account}:network-migration-definition/${NetworkMigrationDefinitionID}	aws:ResourceTag/${TagKey}

Condition keys for AWS Application Migration Service

AWS Application 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 AWS global condition context keys.

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

Condition keys	Description	Type
mgn:CreateAction	Filters access by the name of a resource-creating API action	String

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelPracticeRun	Grants permission to cancel an active practice run	Write	ALB*		

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

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

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

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

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

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

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

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

Resource types defined by Amazon Application Recovery Controller - Zonal Shift

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

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

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

Condition keys for Amazon Application Recovery Controller - Zonal Shift

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

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

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

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

Actions, resources, and condition keys for AWS Application Transformation Service

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

References:

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

Topics

- Actions defined by AWS Application Transformation Service
- Resource types defined by AWS Application Transformation Service
- Condition keys for AWS Application Transformation Service

Actions defined by AWS Application Transformation Service

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContainerization	Grants permission to get the details of all Containerization jobs	Read			
GetDeployment	Grants permission to get the details of all Deployment jobs	Read			
GetGroupingAssessment	Grants permission to Get the details of a Grouping Assessment Operation	Read			
GetPortingCompatibilityAssessment	Grants permission to Get Porting Compatibility Operation	Read			
GetPortingRecommendationAssessment	Grants permission to Get the details of a Porting Recommendation Assessment Operation	Read			
GetRuntimeAssessment	Grants permission to Get the details of a Runtime Assessment Operation	Read			
PutLogData	Grants permission to Push Logs (Intended for Clients Only)	Write			
PutMetricData	Grants permission to Push Metrics Data (Intended for Clients Only)	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartContainerization	Grants permission to start a Containerization job	Write			
StartDeployment	Grants permission to start a Deployment job	Write			
StartGroupingAssessment	Grants permission to Start a Grouping Assessment Operation	Write			
StartPortingCompatibilityAssessment	Grants permission to Start Porting Compatibility Operation	Write			
StartPortingRecommendationAssessment	Grants permission to Start the Porting Recommendation Assessment Operation	Write			
StartRuntimeAssessment	Grants permission to Start a Runtime Assessment Operation	Write			

Resource types defined by AWS Application Transformation Service

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

Condition keys for AWS Application Transformation Service

Application Transformation 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 AWS global condition context keys.

Actions, resources, and condition keys for Amazon AppStream 2.0

Amazon AppStream 2.0 (service prefix: `appstream`) 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 AppStream 2.0
- Resource types defined by Amazon AppStream 2.0
- Condition keys for Amazon AppStream 2.0

Actions defined by Amazon AppStream 2.0

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAppBlockBuilderAppBlock	Grants permission to associate the specified app block builder with the app block	Write	app-block*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
Associate ApplicationFleet	Grants permission to associate the specified application with the fleet	Write	application*		
			fleet*		
				aws:ResourceTag/${TagKey}	
Associate ApplicationToEntitlement	Grants permission to associate the specified application to the specified entitlement	Write	stack*		
Associate Fleet	Grants permission to associate the specified fleet with the specified stack	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateSoftwareToImageBuilder	Grants permission to associate license included application(s) with an existing image builder instance	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
BatchAssociateUserStack	Grants permission to associate the specified users with the specified stacks. Users in a user pool cannot be assigned to stacks with fleets that are joined to an Active Directory domain	Write	stack*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateUserStack	Grants permission to disassociate the specified users from the specified stacks	Write	stack*		
				aws:ResourceTag/${TagKey}	
CopyImage	Grants permission to copy the specified image within the same Region or to a new Region within the same AWS account	Write	image*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppBlock	Grants permission to create an app block. App blocks store details about the virtual hard disk that contains the files for the application in an S3 bucket. It also stores the setup script with details about how to mount the virtual hard disk. App blocks are only supported for Elastic fleets	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilder	Grants permission to create an app block builder. An app block builder is a virtual machine that is used to create an app block	Write	app-block-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppBlockBuilderStreamingURL	Grants permission to create a URL to start an app block builder streaming session	Write	app-block-builder*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an application within customer account. Applications store the details about how to launch applications on streaming instances. This is only supported for Elastic fleets	Write	app-block*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateDirectoryConfig	Grants permission to create a Directory Config object in AppStream 2.0. This object includes the configuration information required to join fleets and image builders to Microsoft Active Directory domains	Write			
CreateEntitlement	Grants permission to create an entitlement to control access to applications based on user attributes	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExportImageTask	Grants permission to create an export task for an AppStream 2.0 image	Write		aws:ResourceTag/${TagKey}	
CreateFleet	Grants permission to create a fleet. A fleet is a group of streaming instances from which applications are launched and streamed to users	Write	fleet*		
			image		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilder	Grants permission to create an image builder. An image builder is a virtual machine that is used to create an image	Write	image*		
			image-builder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageBuilderStreamingURL	Grants permission to create a URL to start an image builder streaming session	Write	image-builder*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
CreateImportedImage	Grants permission to create an AppStream 2.0 image from an imported AMI	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateStack	Grants permission to create a stack to start streaming applications to users. A stack consists of an associated fleet, user access policies, and storage configurations	Write	stack*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStreamingURL	Grants permission to create a temporary URL to start an AppStream 2.0 streaming session for the specified user. A streaming URL enables application streaming to be tested without user setup	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateThemeForStack	Grants permission to create a custom branding theme, which might includes a custom logo, website links, and other branding to display to your users	Write	stack*		
CreateUpdatedImage	Grants permission to update an existing image within customer account	Write	image*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateUsageReportSubscription	Grants permission to create a usage report subscription. Usage reports are generated daily	Write			
CreateUser	Grants permission to create a new user in the user pool	Write			
DeleteAppBlock	Grants permission to delete the specified app block	Write	app-block*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteAppBlockBuilder	Grants permission to delete the specified app block builder and release capacity	Write	app-block-builder*		
				aws:ResourceTag/${TagKey}	
DeleteApplication	Grants permission to delete the specified application	Write	application*		
				aws:ResourceTag/${TagKey}	
DeleteDirectoryConfig	Grants permission to delete the specified Directory Config object from AppStream 2.0. This object includes the configuration information required to join fleets and image builders to Microsoft Active Directory domains	Write			
DeleteEntitlement	Grants permission to delete the specified entitlement	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFleet	Grants permission to delete the specified fleet	Write	fleet*		
				aws:ResourceTag/${TagKey}	
DeleteImage	Grants permission to delete the specified image. An image cannot be deleted when it is in use	Write	image*		
				aws:ResourceTag/${TagKey}	
DeleteImageBuilder	Grants permission to delete the specified image builder and release capacity	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
DeleteImagePermissions	Grants permission to delete permissions for the specified private image	Write	image*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStack	Grants permission to delete the specified stack. After the stack is deleted, the application streaming environment provided by the stack is no longer available to users. Also, any reservations made for application streaming sessions for the stack are released	Write	stack*		
				aws:ResourceTag/${TagKey}	
DeleteThemeForStack	Grants permission to delete a custom branding theme, which might includes a custom logo, website links, and other branding to display to your users	Write	stack*		
DeleteUsageReportSubscription	Grants permission to disable usage report generation	Write			
DeleteUser	Grants permission to delete a user from the user pool	Write			
DescribeAppBlockBuilderAppBlockAssociations	Grants permission to retrieve the associations that are associated with the specified app block builder or app block	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAppBlockBuilders	Grants permission to retrieve a list that describes one or more specified app block builders, if the app block builder names are provided. Otherwise, all app block builders in the account are described	List			
DescribeAppBlocks	Grants permission to retrieve a list that describes one or more specified app blocks, if the app block arns are provided. Otherwise, all app blocks in the account are described	List			
DescribeAppLicenseUsage	Grants permission to retrieve license included application usage information	List			
DescribeApplicationFleetAssociations	Grants permission to retrieve the associations that are associated with the specified application or fleet	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeApplications	Grants permission to retrieve a list that describes one or more specified applications, if the application arns are provided. Otherwise, all applications in the account are described	List			
DescribeDirectoryConfigs	Grants permission to retrieve a list that describes one or more specified Directory Config objects for AppStream 2.0, if the names for these objects are provided. Otherwise, all Directory Config objects in the account are described. This object includes the configuration information required to join fleets and image builders to Microsoft Active Directory domains	List			
DescribeEntitlements	Grants permission to retrieve one or all entitlements for the specified stack	List	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFleets	Grants permission to retrieve a list that describes one or more specified fleets, if the fleet names are provided. Otherwise, all fleets in the account are described	List			
DescribeImageBuilders	Grants permission to retrieve a list that describes one or more specified image builders, if the image builder names are provided. Otherwise, all image builders in the account are described	List			
DescribeImagePermissions	Grants permission to retrieve a list that describes the permissions for shared AWS account IDs on a private image that you own	Read	image*		
DescribeImages	Grants permission to retrieve a list that describes one or more specified images, if the image names or image ARNs are provided. Otherwise, all images in the account are described	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSessions	Grants permission to retrieve a list that describes the streaming sessions for the specified stack and fleet. If a user ID is provided for the stack and fleet, only the streaming sessions for that user are described	List	fleet*		
			stack*		
DescribeSoftwareAssociations	Grants permission to retrieve license included application associations for a specified resource	List	image		
			image-builder		
DescribeStacks	Grants permission to retrieve a list that describes one or more specified stacks, if the stack names are provided. Otherwise, all stacks in the account are described	List			
DescribeThemeForStack	Grants permission to get the custom branding theme information, which might includes a custom logo, website links, and other branding to display to your users	Read	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeUsageReportSubscriptions	Grants permission to retrieve a list that describes one or more usage report subscriptions	List			
DescribeUserStackAssociations	Grants permission to retrieve a list that describes the UserStackAssociation objects	List			
DescribeUsers	Grants permission to retrieve a list that describes users in the user pool	List			
DisableUser	Grants permission to disable the specified user in the user pool. This action does not delete the user	Write			
DisassociateAppBlockBuilderAppBlock	Grants permission to disassociate the specified app block builder with the app block	Write	app-block*		
			app-block-builder*		
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFleet	Grants permission to disassociate the specified application from the specified fleet	Write	application*		
			fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DisassociateApplicationFromEntitlement	Grants permission to disassociate the specified application from the specified entitlement	Write	stack*		
DisassociateFleet	Grants permission to disassociate the specified fleet from the specified stack	Write	fleet*		
			stack*		
				aws:ResourceTag/${TagKey}	
DisassociateSoftwareFromImageBuilder	Grants permission to remove license included application(s) association(s) from an image builder instance	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
EnableUser	Grants permission to enable a user in the user pool	Write			
ExpireSession	Grants permission to immediately stop the specified streaming session	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExportImageTask	Grants permission to retrieve details of a specific export image task	Read			
ListAssociatedFleets	Grants permission to retrieve the name of the fleet that is associated with the specified stack	Read	stack*		
ListAssociatedStacks	Grants permission to retrieve the name of the stack with which the specified fleet is associated	Read	fleet*		
ListEntitledApplications	Grants permission to retrieve the applications that are associated with the specified entitlement	List	stack*		
ListExportImageTasks	Grants permission to list export image tasks	List			
ListTagsForResource	Grants permission to retrieve a list of all tags for the specified AppStream 2.0 resource. The following resources can be tagged: Image builders, images, fleets, and stacks	Read			
StartAppBlockBuilder	Grants permission to start the specified app block builder	Write	app-block-builder*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
StartFleet	Grants permission to start the specified fleet	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StartImageBuilder	Grants permission to start the specified image builder	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
StartSoftwareDeploymentToImageBuilder	Grants permission to initiate license included applications deployment to an image builder instance	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
StopAppBlockBuilder	Grants permission to stop the specified app block builder	Write	app-block-builder*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
StopFleet	Grants permission to stop the specified fleet	Write	fleet*		
				aws:ResourceTag/${TagKey}	
StopImageBuilder	Grants permission to stop the specified image builder	Write	image-builder*		
				aws:ResourceTag/${TagKey}	
Stream	Grants permission to federated users to sign in by using their existing credentials and stream applications from the specified stack	Write	stack*		
				appstream:userId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add or overwrite one or more tags for the specified AppStream 2.0 resource. The following resources can be tagged: Image builders, images, fleets, stacks, app blocks and applications	Tagging	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to disassociate one or more tags from the specified AppStream 2.0 resource	Tagging	app-block		
			app-block-builder		
			application		
			fleet		
			image		
			image-builder		
			stack		
				aws:TagKeys	
UpdateAppBlockBuilder	Grants permission to update a specific app block builder. An app block builder is a virtual machine that is used to create an app block	Write	app-block-builder*		
				aws:ResourceTag/${TagKey}	
UpdateApplication	Grants permission to update the specified fields for the specified application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app-block		
				aws:ResourceTag/${TagKey}	
UpdateDirectoryConfig	Grants permission to update the specified Directory Config object in AppStream 2.0. This object includes the configuration information required to join fleets and image builders to Microsoft Active Directory domains	Write			
UpdateEntitlement	Grants permission to update the specified fields for the specified entitlement	Write	stack*		
UpdateFleet	Grants permission to update the specified fleet. All attributes except the fleet name can be updated when the fleet is in the STOPPED state	Write	fleet*		
			image		
				aws:ResourceTag/${TagKey}	
UpdateImagePermissions	Grants permission to add or update permissions for the specified private image	Write	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateStack	Grants permission to update the specified fields for the specified stack	Write	stack*		
				aws:ResourceTag/${TagKey}	
UpdateThemeForStack	Grants permission to update the custom branding theme information, which might includes a custom logo, website links, and other branding to display to your users	Write	stack*		

Resource types defined by Amazon AppStream 2.0

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
fleet	arn:${Partition}:appstream:${Region}:${Account}:fleet/${FleetName}	aws:ResourceTag/${TagKey}
image	arn:${Partition}:appstream:${Region}:${Account}:image/${ImageName}	aws:ResourceTag/${TagKey}
image-builder	arn:${Partition}:appstream:${Region}:${Account}:image-builder/${ImageBuilderName}	aws:ResourceTag/${TagKey}
stack	arn:${Partition}:appstream:${Region}:${Account}:stack/${StackName}	aws:ResourceTag/${TagKey}
app-block	arn:${Partition}:appstream:${Region}:${Account}:app-block/${AppBlockName}	aws:ResourceTag/${TagKey}
application	arn:${Partition}:appstream:${Region}:${Account}:application/${ApplicationName}	aws:ResourceTag/${TagKey}
app-block-builder	arn:${Partition}:appstream:${Region}:${Account}:app-block-builder/${AppBlockBuilderName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon AppStream 2.0

Amazon AppStream 2.0 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

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

Condition keys	Description	Type
appstream:userId	Filters access by the ID of the AppStream 2.0 user	String
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 presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS AppSync

AWS 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 AWS AppSync
- Resource types defined by AWS AppSync
- Condition keys for AWS AppSync

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateApi	Grants permission to attach a GraphQL API to a custom domain name in AppSync	Write	domain*		
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*		
AssociateWebACL [permission only]	Grants permission to associate a web ACL and a resource	Write	api 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			

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey}	
DeleteApiCache	Grants permission to delete an API cache in AppSync	Write			
DeleteApiKey	Grants permission to delete an API key	Write			
DeleteChannelNamespace	Grants permission to delete a channel namespace	Write	channelNamespace*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Grants permission to delete a data source	Write			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DisassociateWebACL [permission only]	Grants permission to disassociate a web ACL and a resource	Write	api		
			graphqlapi		
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*		
EventPublish	Grants permission to publish events to a channel namespace	Write	channelNamespace*		
EventSubscribe	Grants permission to subscribe to a channel namespace	Write	channelNamespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
GetDataSource	Grants permission to retrieve a data source	Read			
GetDataSourceIntrospection	Grants permission to retrieve a data source introspection	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetResolver	Grants permission to retrieve a resolver	Read			
GetResourcePolicy [permission only]	Grants permission to read a resource policy	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetWebACLForResource [permission only]	Grants permission to get associated web ACLs for a resource	Read	api graphqlapi		
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}	
ListChannelNamespaces	Grants permission to list channel namespace	List	api*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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			
ListResourcesForWebACL [permission only]	Grants permission to get associated resources for a web ACL	List			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy [permission only]	Grants permission to set a resource policy	Write			
SetWebACL	Grants permission to set a web ACL	Permissions management			
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		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApi	Grants permission to update an API	Write	api*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDomainName	Grants permission to update a custom domain name in AppSync	Write	domain*		
				aws:ResourceTag/${TagKey}	
UpdateFunction	Grants permission to update an existing function	Write			
UpdateGraphqlApi	Grants permission to update a GraphQL API	Write	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${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 AWS 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}	

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

Condition keys for AWS AppSync

AWS 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 AWS 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 ARC Region switch

Amazon ARC Region switch (service prefix: arc-region-switch) 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 ARC Region switch

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApprovePlanExecutionStep	Grants permission to approve a plan execution step	Write	plan*		
CancelPlanExecution	Grants permission to cancel a plan execution	Write	plan*		
CreatePlan	Grants permission to create a plan	Write	plan*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
DeletePlan	Grants permission to delete a plan	Write	plan*		
DeleteResourcePolicy [permission only]	Grants permission to delete the RAM access control policy for a plan	Permissions management			
GetPlan	Grants permission to get information about plans in all AWS Regions using a control plane	Read	plan*		
GetPlanEvaluationStatus	Grants permission to get a plan's evaluation status	Read	plan*		
GetPlanExecution	Grants permission to get plan execution details and setup information	Read	plan*		
GetPlanInRegion	Grants permission to get information about a plan in a specific AWS Region using the Region switch Regional data plane	Read	plan*		
GetResourcePolicy [permission only]	Grants permission to get the resource policy of a plan	Permissions management	plan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPlanExecutionEvents	Grants permission to list plan execution events	List	plan*		
ListPlanExecutions	Grants permission to list plan executions	List	plan*		
ListPlans	Grants permission to list plans in all AWS Regions using a control plane	List			
ListPlansInRegion	Grants permission to list plans in a specific AWS Region using the Region switch Regional data plane	List			
ListRoute53HealthChecks	Grants permission to list Route 53 health checks	List	plan*		
ListRoute53HealthChecksInRegion	Grants permission to list Route 53 health checks in a specific AWS Region using the Region switch Regional data plane	List	plan*		
ListTagsForResource	Grants permission to list tags for a resource	Read	plan*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy [permission only]	Grants permission to define the RAM access control policy for a plan	Permissions management			
StartPlanExecution	Grants permission to start a plan execution	Write	plan*		
TagResource	Grants permission to tag a resource	Tagging	plan*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	plan*	aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePlan	Grants permission to update a plan	Write	plan*		
UpdatePlanExecution	Grants permission to update a plan execution	Write	plan*		
UpdatePlanExecutionStep	Grants permission to update a plan execution step	Write	plan*		

Resource types defined by Amazon ARC Region switch

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
plan	`arn:${Partition}:arc-region-switch::${Account}:plan/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon ARC Region switch

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

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

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

Actions, resources, and condition keys for AWS Artifact

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

References:

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

Topics

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

Actions defined by AWS Artifact

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

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

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

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

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

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

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

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

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

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

Resource types defined by AWS Artifact

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

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

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

Condition keys for AWS Artifact

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

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

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

Actions, resources, and condition keys for 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

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

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS services and principals that use Athena JDBC driver earlier than 1.1.0. Use StopQuery Execution otherwise	Write	workgroup*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	Grants permission to create a named query	Write	workgroup*		
CreateNotebook	Grants permission to create a notebook	Write	workgroup*		
CreatePreparedStatement	Grants permission to create a prepared statement	Write	workgroup*		
CreatePresignedNotebookUrl	Grants permission to create a presigned notebook url	Write	workgroup*		
CreateWorkGroup	Grants permission to create a workgroup	Write	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
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 AWS 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
GetExecutionEngines	Grants permission to enable access to databases and tables. Applies only to AWS 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*		
GetNamespace	Grants permission to enable access to the specified database and table. Applies only to AWS 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 AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQueryExecution	Grants permission to get information about the specified query execution	Read	workgroup *		
GetQueryExecutions	Grants permission to get query executions. Deprecated. Applies only to AWS 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 *		
GetResourceDashboard	Grants permission to get a Live UI/Persistence UI for a session	Read	workgroup *		
			session		
GetSession	Grants permission to get a session	Read	workgroup *		
			session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSessionEndpoint	Grants permission to get a connection endpoint and authentication token for a given session Id	Write	workgroup*		
			session		
GetSessionStatus	Grants permission to get a session status	Read	workgroup*		
			session		
GetTable	Grants permission to enable access to the specified table. Applies only to AWS services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
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 AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account	List			
ListDataCatalogs	Grants permission to return a list of datacatalogs for the specified AWS 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 AWS 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 AWS account	List	workgroup*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workgroup*		
ListWorkGroups	Grants permission to return a list of workgroups for the specified AWS account	List			
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 AWS 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*		
			session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
StopCalculationExecution	Grants permission to stop a calculation execution	Write	workgroup*		
StopQueryExecution	Grants permission to stop the specified query execution	Write	workgroup*		
TagResource	Grants permission to add a tag to a resource	Tagging	capacity-reservation*		
			datacatalog*		
			session*		
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

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

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

Resource types	ARN	Condition keys
session	arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}/session/${SessionId}	aws:ResourceTag/${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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 AWS Audit Manager

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

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Audit Manager

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

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

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

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

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAssessmentReportEvidenceFolder	Grants permission to associate an evidence folder with an assessment report in AWS Audit Manager	Write	assessment*		
BatchAssociateAssessmentReportEvidence	Grants permission to associate a list of evidence to an assessment report in AWS Audit Manager	Write	assessment*		
BatchCreateDelegationByAssessment	Grants permission to create delegations for an assessment in AWS Audit Manager	Write	assessment* assessmentControlSet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteDelegationByAssessment	Grants permission to delete delegations for an assessment in AWS Audit Manager	Write	assessment*		
			assessmentControlSet*		
BatchDisassociateAssessmentReportEvidence	Grants permission to disassociate a list of evidence from an assessment report in AWS Audit Manager	Write	assessment*		
BatchImportEvidenceToAssessmentControl	Grants permission to import a list of evidence to an assessment control in AWS Audit Manager	Write	assessmentControlSet*		
CreateAssessment	Grants permission to create an assessment to be used with AWS Audit Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAssessmentFramework	Grants permission to create a framework for use in AWS Audit Manager	Write	assessmentFramework*		
			control*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateAssessmentReport	Grants permission to create an assessment report in AWS Audit Manager	Write	assessment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateControl	Grants permission to create a control to be used in AWS Audit Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAssessment	Grants permission to delete an assessment in AWS Audit Manager	Write	assessment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFramework	Grants permission to delete an assessment framework in AWS Audit Manager	Write	assessmentFramework*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAssessmentFrameworkShare	Grants permission to delete a share request for a custom framework in AWS Audit Manager	Write			
DeleteAssessmentReport	Grants permission to delete an assessment report in AWS Audit Manager	Write	assessment*		
DeleteControl	Grants permission to delete a control in AWS Audit Manager	Write	control*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeregisterAccount	Grants permission to deregister an account in AWS Audit Manager	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterOrganizationAdminAccount	Grants permission to deregister the delegated administrator account for AWS Audit Manager	Write			
DisassociateAssessmentReportEvidenceFolder	Grants permission to disassociate an evidence folder from an assessment report in AWS Audit Manager	Write	assessment*		
GetAccountStatus	Grants permission to get the status of an account in AWS Audit Manager	Read			
GetAssessment	Grants permission to get an assessment created in AWS Audit Manager	Read	assessment*		
GetAssessmentFramework	Grants permission to get an assessment framework in AWS Audit Manager	Read	assessmentFramework*		
GetAssessmentReportUrl	Grants permission to get the URL for an assessment report in AWS Audit Manager	Read	assessment*		
GetChangeLogs	Grants permission to get changelogs for an assessment in AWS Audit Manager	Read	assessment*		
GetControl	Grants permission to get a control in AWS Audit Manager	Read	control*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDelegations	Grants permission to get all delegations in AWS Audit Manager	List			
GetEvidence	Grants permission to get evidence from AWS Audit Manager	Read	assessmentControlSet*		
GetEvidenceByEvidenceFolder	Grants permission to get all the evidence from an evidence folder in AWS Audit Manager	Read	assessmentControlSet*		
GetEvidenceFileUploadUrl	Grants permission to get a presigned Amazon S3 URL that can be used to upload a file as manual evidence	Read			
GetEvidenceFolder	Grants permission to get the evidence folder from AWS Audit Manager	Read	assessmentControlSet*		
GetEvidenceFoldersByAssessment	Grants permission to get the evidence folders from an assessment in AWS Audit Manager	Read	assessment*		
GetEvidenceFoldersByAssessmentControl	Grants permission to get the evidence folders from an assessment control in AWS Audit Manager	Read	assessmentControlSet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInsights	Grants permission to get analytics data for all active assessments	Read			
GetInsightsByAssessment	Grants permission to get analytics data for a specific active assessment	Read			
GetOrganizationAdminAccount	Grants permission to get the delegated administrator account in AWS Audit Manager	Read			
GetServicesInScope	Grants permission to get the services in scope for an assessment in AWS Audit Manager	Read			
GetSettings	Grants permission to get all settings configured in AWS Audit Manager	Read			
ListAssessmentControlInsightsByControlDomain	Grants permission to list analytics data for controls in a specific control domain and active assessment	List			
ListAssessmentFrameworkShareRequests	Grants permission to list all sent or received share requests for custom frameworks in AWS Audit Manager	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssessmentFrameworks	Grants permission to list all assessment frameworks in AWS Audit Manager	List			
ListAssessmentReports	Grants permission to list all assessment reports in AWS Audit Manager	List			
ListAssessments	Grants permission to list all assessments in AWS Audit Manager	List			
ListControlDomainInsights	Grants permission to list analytics data for control domains across all active assessments	List			
ListControlDomainInsightsByAssessment	Grants permission to list analytics data for control domains in a specific active assessment	List			
ListControlInsightsByControlDomain	Grants permission to list analytics data for controls in a specific control domain across all active assessments	List			
ListControls	Grants permission to list all controls in AWS Audit Manager	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListKeywordsForDataSource	Grants permission to list all the data source keywords in AWS Audit Manager	List			
ListNotifications	Grants permission to list all notifications in AWS Audit Manager	List			
ListTagsForResource	Grants permission to list tags for an AWS Audit Manager resource	Read	assessment		
			control		
RegisterAccount	Grants permission to register an account in AWS Audit Manager	Write			
RegisterOrganizationAdminAccount	Grants permission to register an account within the organization as the delegated administrator for AWS Audit Manager	Write			
StartAssessmentFrameworkShare	Grants permission to create a share request for a custom framework in AWS Audit Manager	Write	assessmentFramework*		
TagResource	Grants permission to tag an AWS Audit Manager resource	Tagging	assessment		
			assessmentFramework		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			control		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag an AWS Audit Manager resource	Tagging	assessment	aws:ResourceTag/${TagKey}	
			assessmentFramework	aws:ResourceTag/${TagKey}	
			control	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAssessment	Grants permission to update an assessment in AWS Audit Manager	Write	assessment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAssessmentControl	Grants permission to update an assessment control in AWS Audit Manager	Write	assessmentControlSet*		
UpdateAssessmentControlSetStatus	Grants permission to update the status of an assessment control set in AWS Audit Manager	Write	assessmentControlSet*		
UpdateAssessmentFramework	Grants permission to update an assessment framework in AWS Audit Manager	Write	assessmentFramework*		
			control*		
UpdateAssessmentFrameworkShare	Grants permission to update a share request for a custom framework in AWS Audit Manager	Write	assessmentFramework*		
UpdateAssessmentStatus	Grants permission to update the status of an assessment in AWS Audit Manager	Write	assessment*		
UpdateControl	Grants permission to update a control in AWS Audit Manager	Write	control*		
UpdateSettings	Grants permission to update settings in AWS Audit Manager	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateAssessmentReportIntegrity	Grants permission to validate the integrity of an assessment report in AWS Audit Manager	Read			

Resource types defined by AWS Audit 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
assessment	`arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}`	aws:ResourceTag/${TagKey}
assessmentFramework	`arn:${Partition}:auditmanager:${Region}:${Account}:assessmentFramework/${AssessmentFrameworkId}`	aws:ResourceTag/${TagKey}
assessmentControlSet	`arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${AssessmentId}/controlSet/${ControlSetId}`	
control	`arn:${Partition}:auditmanager:${Region}:${Account}:control/${ControlId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Audit Manager

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

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

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

Amazon Aurora DSQL (service prefix: `dsql`) 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 Aurora DSQL
- Resource types defined by Amazon Aurora DSQL
- Condition keys for Amazon Aurora DSQL

Actions defined by Amazon Aurora DSQL

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPeerCluster [permission only]	Grants permission to add a peer cluster to a multi-Region cluster	Write	Cluster*		dsql:PutMultiRegionProperties
CreateCluster	Grants permission to create new clusters	Write	Cluster*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys dsql:WitnessRegion	
DbConnect	Grants permission to connect to the database	Write	Cluster*		
DbConnectAdmin	Grants permission to connect to the database with admin role. Connecting with any	Write	Cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	other role requires DbConnect permission				
DeleteCluster	Grants permission to delete a cluster and all of its data	Write	Cluster*		
DeleteClusterPolicy	Grants permission to remove the inline resource-based policy attached to a cluster	Write	Cluster*		
GetBackupJob	Grants permission to get the status of an Aurora DSQL cluster backup job	Read	Cluster*		
GetCluster	Grants permission to get information about a cluster	Read	Cluster*		
GetClusterPolicy	Grants permission to retrieve the inline resource-based policy attached to a cluster	Read	Cluster*		
GetRestoreJob	Grants permission to get the status of an Aurora DSQL cluster restore job	Read	Cluster*		
GetVpcEndpointServiceName	Grants permission to retrieve the VPC endpoint service name for a cluster	Read	Cluster*		
InjectError [permission only]	Grants permission to inject errors in targeted clusters	Write		dsql:FisActionId dsql:FisTargetArns	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClusters	Grants permission to retrieve a list of clusters	List			
ListTagsForResource	Grants permission to list all tags on an Aurora DSQL resource	Read	Cluster*		
PutClusterPolicy	Grants permission to attach or update the inline resource-based policy attached to a cluster	Write	Cluster*		
PutMultiRegionProperties [permission only]	Grants permission to update multi-Region properties of a cluster	Write	Cluster*		
PutWitnessRegion [permission only]	Grants permission to configure and update the witness Region of a multi-Region cluster	Write	Cluster*		dsql:PutMultiRegionProperties
				dsql:WitnessRegion	
RemovePeerCluster [permission only]	Grants permission to remove a peer cluster from a multi-Region cluster	Write	Cluster*		dsql:PutMultiRegionProperties

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartBackupJob	Grants permission to start a backup job for an Aurora DSQL cluster	Write	Cluster*		
StartRestoreJob	Grants permission to start a restore job for an Aurora DSQL cluster	Write	Cluster*		dsql:CreateCluster iam:CreateServiceLinkedRole
StopBackupJob	Grants permission to stop a backup job for an Aurora DSQL cluster	Write	Cluster*		
StopRestoreJob	Grants permission to stop a restore job for an Aurora DSQL Cluster	Write	Cluster*		
TagResource	Grants permission to add tags to Aurora DSQL resources	Tagging	Cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from Aurora DSQL resources	Tagging	Cluster*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	Grants permission to modify cluster attributes	Write	Cluster*		
				dsql:WitnessRegion	

Resource types defined by Amazon Aurora DSQL

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:${Partition}:dsql:${Region}:${Account}:cluster/${Identifier}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Aurora DSQL

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

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

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
dsql:FisActionId	Filters access by the ID of an AWS FIS action	String
dsql:FisTargetArns	Filters access by the ARN of an AWS FIS target	ArrayOfARN
dsql:WitnessRegion	Filters access by the witness region of multi-Region clusters	String

Actions, resources, and condition keys for AWS Auto Scaling

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

References:

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

Topics

- Actions defined by AWS Auto Scaling
- Resource types defined by AWS Auto Scaling
- Condition keys for AWS Auto Scaling

Actions defined by AWS Auto Scaling

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateScalingPlan	Creates a scaling plan.	Write			
DeleteScalingPlan	Deletes the specified scaling plan.	Write			
DescribeScalingPlanResources	Describes the scalable resources in the specified scaling plan.	Read			
DescribeScalingPlans	Describes the specified scaling plans or all of your scaling plans.	Read			
GetScalingPlanResourceForecastData	Retrieves the forecast data for a scalable resource.	Read			
UpdateScalingPlan	Updates a scaling plan.	Write			

Resource types defined by AWS Auto Scaling

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

Condition keys for AWS Auto Scaling

Auto Scaling has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS B2B Data Interchange

AWS B2B Data Interchange (service prefix: `b2bi`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

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

Topics

Actions defined by AWS B2B Data Interchange

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapability	Grants permission to create a capability	Write	transformer		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
CreatePartnership	Grants permission to create a partnership	Write	capability*		
			profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile	Grants permission to create a profile	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateStarterMappingTemplate	Grants permission to generate a starter JSONATA/XSLT template	Write	transformer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransformer	Grants permission to create a transformer	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCapability	Grants permission to delete a capability	Write	capability*		
DeletePartnership	Grants permission to delete an partnership	Write	partnership*		
DeleteProfile	Grants permission to delete a profile	Write	profile*		
DeleteTransformer	Grants permission to delete a transformer	Write	transformer*		
GenerateMapping	Grants permission to generate a starter JSONATA/XSLT mapping template from Amazon Bedrock	Write	transformer*		
GetCapability	Grants permission to get a capability	Read	capability*		
GetPartnership	Grants permission to get a partnership	Read	partnership*		
GetProfile	Grants permission to get a profile	Read	profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransformer	Grants permission to get a transformer	Read	transformer*		
GetTransformerJob	Grants permission to get a transformer job	Read	transformer*		
ListCapabilities	Grants permission to list all capabilities	List			
ListPartnerships	Grants permission to list all partnerships	List			
ListProfiles	Grants permission to list all profiles	List			
ListTagsForResource	Grants permission to list tags for a B2Bi resource	Read	capability		
			partnership		
			profile		
			transformer		
ListTransformers	Grants permission to list all transformers	List			
StartTransformerJob	Grants permission to transformer a document	Write	transformer*		
TagResource	Grants permission to tag a B2Bi resource	Tagging	capability		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			partnership		
			profile		
			transformer		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConversion	Grants permission to convert a JSON/XML to an edi document	Write	transformer*		
TestMapping	Grants permission to map a sample file	Write	transformer*		
TestParsing	Grants permission to parse an edi document	Write	transformer*		
UntagResource	Grants permission to untag a B2Bi resource	Tagging	capability		
			partnership		
			profile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transformer		
				aws:TagKeys	
UpdateCapability	Grants permission to update a capability	Write	capability*		
			transformer		
UpdatePartnership	Grants permission to update a partnership	Write	partnership*		
			capability		
UpdateProfile	Grants permission to update a profile	Write	profile*		
UpdateTransformer	Grants permission to update a transformer	Write	transformer*		

Resource types defined by AWS B2B Data Interchange

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:${Partition}:b2bi:${Region}:${Account}:profile/${ResourceId}	aws:ResourceTag/${TagKey}
capability	arn:${Partition}:b2bi:${Region}:${Account}:capability/${ResourceId}	aws:ResourceTag/${TagKey}
partnership	arn:${Partition}:b2bi:${Region}:${Account}:partnership/${ResourceId}	aws:ResourceTag/${TagKey}
transformer	arn:${Partition}:b2bi:${Region}:${Account}:transformer/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS B2B Data Interchange

AWS B2B Data Interchange defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

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

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

Actions, resources, and condition keys for AWS Backup

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

References:

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

Topics

Actions defined by AWS Backup

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Resource types defined by AWS Backup

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

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

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

Condition keys for AWS Backup

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

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

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

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

Actions, resources, and condition keys for AWS Backup Gateway

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

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

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

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

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Backup Search

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

References:

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

Topics

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

Actions defined by AWS Backup Search

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSearchJob	Grants permission to get details of a search job	Read	searchJob*		
GetSearchResultExportJob	Grants permission to get details of a search result export job	Read	searchExportJob*		
ListSearchJobBackups	Grants permission to list backups in scope of a search job	Read	searchJob*		
ListSearchJobResults	Grants permission to list results of a search job	Read	searchJob*		
ListSearchJobs	Grants permission to list search jobs	List			
ListSearchResultExportJobs	Grants permission to list search result export jobs	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	searchExportJob		
			searchJob		
StartSearchJob	Grants permission to create a search job	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StartSearchResultExportJob	Grants permission to start an export job for an existing search job	Write	searchJob*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StopSearchJob	Grants permission to stop an in-progress search job	Write	searchJob*		
TagResource	Grants permission to tag a resource	Tagging	searchExportJob		
			searchJob		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	searchExportJob		
			searchJob		
				aws:TagKeys	

Resource types defined by AWS Backup Search

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
searchJob	`arn:${Partition}:backup-search:${Region}:${Account}:search-job/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
searchExportJob	arn:${Partition}:backup-search:${Region}:${Account}:search-export-job/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Backup Search

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

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

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

Actions, resources, and condition keys for AWS Backup storage

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	Grants permission to get base backup	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutChunk [permission only]	Grants permission to upload data to an AWS 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 AWS Backup-managed recovery point for a backup job	Write			
UpdateObjectComplete [permission only]	Grants permission to update object complete	Write			

Resource types defined by AWS Backup storage

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

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Batch

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

References:

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

Topics

Actions defined by AWS Batch

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys batch:SchedulingPriority	
TagResource	Grants permission to tag an AWS Batch resource in your account	Tagging	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			quota-share		

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConsumableResource	Grants permission to update an AWS Batch consumable resource in your account	Write	consumable-resource*		
UpdateJobQueue	Grants permission to update an AWS Batch job queue in your account	Write	job-queue*		
			compute-environment		
			scheduling-policy		
UpdateQuotaShare	Grants permission to update an AWS Batch quota share in your account	Write	quota-share*		
UpdateSchedulingPolicy	Grants permission to update an AWS Batch scheduling policy in your account	Write	scheduling-policy*		
UpdateServiceEnvironment	Grants permission to update an AWS Batch service environment in your account	Write	service-environment*		
UpdateServiceJob	Grants permission to update a service job in an AWS Batch job queue in your account	Write	service-job*		
				batch:SchedulingPriority	

Resource types defined by AWS Batch

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

Resource types	ARN	Condition keys
compute-environment	`arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}`	aws:ResourceTag/${TagKey}
job-queue	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}`	aws:ResourceTag/${TagKey}
job-definition	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}`	
job-definition-revision	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:batch:${Region}:${Account}:job/${JobId}`	aws:ResourceTag/${TagKey}
scheduling-policy	`arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}`	aws:ResourceTag/${TagKey}
service-environment	`arn:${Partition}:batch:${Region}:${Account}:service-environment/${ServiceEnvironmentName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
service-job	arn:${Partition}:batch:${Region}:${Account}:service-job/${JobId}	aws:ResourceTag/${TagKey}
consumable-resource	arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}	aws:ResourceTag/${TagKey}
quota-share	arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}/quota-share/${QuotaShareName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Batch

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

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

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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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:SchedulingPriority	Filters access by the scheduling priority for jobs in the job queue	Numeric
batch:ShareIdentifier	Filters access by the shareIdentifier used inside submit job	String
batch:User	Filters access by user name or numeric uid used inside the container	String

Actions, resources, and condition keys for Amazon Bedrock

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

References:

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

Topics

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

Actions defined by Amazon Bedrock

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CallWithBearerToken	Grants permission to use bearer token	Read		bedrock:BearerTokenType	
CancelAutomatedReasoningPolicyBuildWorkflow	Grants permission to cancel a build workflow for an automated reasoning policy	Write	automated-reasoning-policy*		
CopyBlueprintStage	Grants permission to copy a blueprint from one stage to another	Write	blueprint*		
CountTokens	Grants permission to count the number of tokens in an input prompt	Read	foundation-model*		
CreateAgent	Grants permission to create a new agent and a test agent alias pointing to the DRAFT agent version	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentActionGroup	Grants permission to create a new action group in an existing agent	Write	agent*		

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAutomatedReasoningPolicyNextScenario	Grants permission to retrieve the next unreviewed generated scenario for a build workflow for an automated reasoning policy	Read	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestCase	Grants permission to retrieve a test case for an automated reasoning policy	Read	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestResult	Grants permission to retrieve result for a test case for an automated reasoning policy	Read	automated-reasoning-policy*		
GetBlueprint	Grants permission to retrieve an existing blueprint for data automation	Read	blueprint*		
GetBlueprintOptimizationStatus	Grants permission to get the status of a blueprint optimization job	Read	blueprint-optimization-invocation*		
GetBlueprintRecommendation [permission only]	Grants permission to retrieve blueprint recommendation	Read			

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSession	Grants permission to retrieve an existing session	Read	session*		
GetUseCaseForModelAccess	Grants permission to retrieve a use case for model access	Read			
IngestKnowledgeBaseDocuments	Grants permission to directly ingest documents into a knowledge base	Write	knowledge-base*		
InvokeAgent	Grants permission to send user input (text-only) to the alias of an agent for Bedrock	Read	agent-alias*		
InvokeAutomatedReasoningPolicy [permission only]	Grants permission to invoke an Automated Reasoning policy	Read	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
InvokeBlueprintOptimizationAsync	Grants permission to invoke an async job to perform blueprint optimization	Write	blueprint*		
			data-automation-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeBlueprintRecommendationAsync [permission only]	Grants permission to invoke blueprint recommendations asynchronously	Write	data-automation-profile*		
InvokeBuilder [permission only]	Grants permission to use the conversational builder which aids in building supported bedrock resources	Write			
InvokeDataAutomation	Grants permission to invoke a call to Sync API of Bedrock data automation	Write	blueprint*		
			data-automation-profile*		
			data-automation-project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvokeDataAutomationAsync	Grants permission to invoke a Bedrock data automation job	Write	blueprint*		
			data-automation-profile*		
			data-automation-project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeFlow	Grants permission to invoke a prompt flow with user input	Read	flow-alias*		
InvokeInlineAgent	Grants permission to send user input (text-only) to the inline agent for Bedrock	Read		bedrock:InlineAgentName	
InvokeModel	Grants permission to invoke the specified Bedrock model to run inference using the input provided in the request body	Read	application-inference-profile*		

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to Untag a Bedrock resource	Tagging	agent		
			agent-alias		
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			blueprint-optimization-invocation		
			custom-model		
			custom-model-deployment		
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFlowAlias	Grants permission to update the configuration of an alias of a prompt flow	Write	flow-alias*		
UpdateGuardrail	Grants permission to update a guardrail	Write	guardrail*		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
UpdateKnowledgeBase	Grants permission to update a knowledge base	Write	knowledge-base*		
UpdateMarketplaceModelEndpoint	Grants permission to update a marketplace model endpoint	Write	bedrock-marketplace-model-endpoint*		
UpdatePrompt	Grants permission to update a prompt	Write	prompt*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProvisionedModelThroughput	Grants permission to update a provisioned model throughput that you created earlier	Write	custom-model*		
			foundation-model*		
			provisioned-model*		
UpdateSession	Grants permission to update an existing session	Write	session*		
ValidateFlowDefinition	Grants permission to validate prompt flow definitions	Read			

Resource types defined by Amazon Bedrock

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

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

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

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

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

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

Condition keys for Amazon Bedrock

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

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

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

Actions, resources, and condition keys for Amazon Bedrock Agentcore

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

References:

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

Topics

Actions defined by Amazon Bedrock Agentcore

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended telemetry for a resource	Permissions management	memory*		
AuthorizeAction	Grants permission to evaluate Cedar policies for authorization requests	Permissions	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]		management	policy-engine*		
BatchCreateMemoryRecords	Grants permission to create one or more memory records	Write	memory*		
				bedrock-agentcore:namespace	
BatchDeleteMemoryRecords	Grants permission to delete one or more memory records	Write	memory*		
BatchUpdateMemoryRecords	Grants permission to update one or more memory records	Write	memory*		
				bedrock-agentcore:namespace	
CompleteResourceTokenAuth	Grants permission to retrieve access token with OAuth2 for 3LO flow to access external resource	Read	oauth2credentialprovider*		
			token-vault*		
			workload-identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workload-identity-directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				bedrock-agentcore:InboundJwtClaim/iss bedrock-agentcore:InboundJwtClaim/sub bedrock-agentcore:InboundJwtClaim/aud bedrock-agentcore:InboundJwtClaim/scope bedrock-agentcore:InboundJw	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tClaim/client_id bedrock-agentcore:userid	
ConnectBrowserAutomationStream	Grants permission to connect to a browser automation stream	Read			
ConnectBrowserLiveViewStream	Grants permission to connect to a browser live view stream	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAgentRuntime	Grants permission to create a new agent runtime	Write		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:subnets bedrock-agentcore:securityGroups	iam:PassRole
CreateAgentRuntimeEndpoint	Grants permission to create a new agent runtime endpoint	Write	runtime*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApiKeyCredentialProvider	Grants permission to create a new API Key Credential Provider	Write	apikeycredentialprovider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			token-vault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrowser	Grants permission to create a new custom browser	Write		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:subnets bedrock-agentcore:securityGroups	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBrowserProfile	Grants permission to create a new browser profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeInterpreter	Grants permission to create a new custom code interpreter	Write		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:subnets bedrock-agentcore:securityGroups	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEvaluator	Grants permission to create a new evaluator	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateEvent	Grants permission to create an Event	Write	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
CreateGateway	Grants permission to create a new gateway	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGatewayTarget	Grants permission to create a new target in an existing gateway	Write	gateway*		
CreateMemory	Grants permission to create a Memory resource	Write		aws:RequestTag/${TagKey} aws:TagKeys bedrock-agentcore:KmsKeyArn	iam:PassRole
CreateOauth2CredentialProvider	Grants permission to create a new Credential Provider to access external resources with OAuth2 protocol	Write	oauth2credentialprovider*		
			token-vault*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOnlineEvaluationConfig	Grants permission to create a new online evaluation configuration	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
CreatePolicy	Grants permission to create a new policy within a policy engine	Write	policy-engine*		
CreatePolicyEngine	Grants permission to create a new policy engine	Write			
CreateWorkloadIdentity	Grants permission to create a new Workload Identity	Write	workload-identity*		
			workload-identity-directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgentRuntime	Grants permission to delete an agent runtime	Write	runtime*		
DeleteAgentRuntimeEndpoint	Grants permission to delete an agent runtime endpoint	Write	runtime*		
			runtime-endpoint*		
DeleteApiKeyCredentialProvider	Grants permission to delete a registered API Key Credential Provider	Write	apikeycredentialprovider*		
			token-vault*		
DeleteBrowser	Grants permission to delete a custom browser	Write	browser-custom*		
DeleteBrowserProfile	Grants permission to delete a browser profile	Write	browser-profile*		
DeleteCodeInterpreter	Grants permission to delete a custom code interpreter	Write	code-interpreter-custom*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEvaluator	Grants permission to delete an evaluator	Write	evaluator*		
DeleteEvent	Grants permission to delete an Event	Write	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
DeleteGateway	Grants permission to delete an existing gateway	Write	gateway*		
DeleteGatewayTarget	Grants permission to delete an existing gateway target	Write	gateway*		
DeleteMemory	Grants permission to delete a Memory resource	Write	memory*		
DeleteMemoryRecord	Grants permission to delete a Memory Record	Write	memory*		
DeleteOauth2CredentialProvider	Grants permission to delete a registered OAuth2 Credential Provider	Write	oauth2credentialprovider*		
			token-vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOnlineEvaluationConfig	Grants permission to delete an online evaluation configuration	Write	online-evaluation-config*		
DeletePolicy	Grants permission to delete a policy	Write	policy*		
			policy-engine*		
DeletePolicyEngine	Grants permission to delete a policy engine	Write	policy-engine*		
DeleteResourcePolicy	Grants permission to delete the resource-based policy for a Bedrock resource	Write	gateway		
			runtime		
			runtime-endpoint		
DeleteWorkloadIdentity	Grants permission to delete a registered Workload Identity	Write	workload-identity*		
			workload-identity-directory*		
Evaluate	Grants permission to run an evaluation using an evaluator	Write	evaluator*		
GetAgentCard	Grants permission to retrieve an agent card for A2A	Read	runtime*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			runtime-endpoint*		
GetAgentRuntime	Grants permission to get details of an agent runtime	Read	runtime*		
GetAgentRuntimeEndpoint	Grants permission to get details of an agent runtime endpoint	Read	runtime*		
			runtime-endpoint*		
GetApiKeyCredentialProvider	Grants permission to fetch a registered API Key Credential Provider by its name	Read	apikeycredentialprovider*		
			token-vault*		
GetBrowser	Grants permission to get details of a browser	Read	browser-custom*		
GetBrowserProfile	Grants permission to get details of a browser profile	Read	browser-profile*		
GetBrowserSession	Grants permission to get details of a browser session	Read	browser*		
			browser-custom*		
GetCodeInterpreter	Grants permission to get details of a code interpreter	Read	code-interpreter-custom*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCodeInterpreterSession	Grants permission to get details of a code interpreter session	Read	code-interpreter*		
			code-interpreter-custom*		
GetEvaluator	Grants permission to get details of an evaluator	Read	evaluator*		
GetEvent	Grants permission to fetch an Event	Read	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
GetGateway	Grants permission to retrieve an existing gateway	Read	gateway*		
GetGatewayTarget	Grants permission to retrieve an existing gateway target	Read	gateway*		
GetMemory	Grants permission to fetch details for a Memory resource	Read	memory*		
GetMemoryRecord	Grants permission to fetch a Memory Record	Read	memory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOauth2CredentialProvider	Grants permission to fetch a registered OAuth2 Credential Provider by its name	Read	oauth2credentialprovider*		
			token-vault*		
GetOnlineEvaluationConfig	Grants permission to get details of an online evaluation configuration	Read	online-evaluation-config*		
GetPolicy	Grants permission to retrieve a policy	Read	policy*		
			policy-engine*		
GetPolicyEngine	Grants permission to retrieve a policy engine	Read	policy-engine*		
GetPolicyGeneration	Grants permission to retrieve status and results of a policy generation request	Read	policy-engine*		
			policy-generation*		
GetResourceApiKey	Grants permission to retrieve an API Key associated with an Api Key Credential Provider	Read	apikeycredentialprovider*		
			token-vault*		
			workload-identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workload-identity-directory*		
GetResourceOauth2Token	Grants permission to retrieve access token with OAuth2 2LO or 3LO flow to access external resource	Read	oauth2credentialprovider*		
			token-vault*		
			workload-identity*		
			workload-identity-directory*		
GetResourcePolicy	Grants permission to retrieve the resource-based policy for a Bedrock resource	Read	gateway		
			runtime		
			runtime-endpoint		
GetTokenVault	Grants permission to fetch the current configuration of the TokenVault, including encryption settings	Read	token-vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWorkloadAccessToken	Grants permission to retrieve an Workload access token for agentic workloads not acting on behalf of a user	Write	workload-identity*		
			workload-identity-directory*		
GetWorkloadAccessTokenForJWT	Grants permission to retrieve an Workload access token for agentic workloads acting on behalf of user with JWT token	Write	workload-identity*		
			workload-identity-directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				bedrock-agentcore:InboundJwtClaim/iss bedrock-agentcore:InboundJwtClaim/sub bedrock-agentcore:InboundJwtClaim/aud bedrock-agentcore:InboundJwtClaim/scope bedrock-agentcore:InboundJw	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tClaim/client_id	
GetWorkloadAccessTokenForUserId	Grants permission to retrieve an Workload access token for agentic workloads acting on behalf of user with User Id	Write	workload-identity*		
			workload-identity-directory*		
				bedrock-agentcore:userid	
GetWorkloadIdentity	Grants permission to fetch details for a specific Workload identity, including its name and allowed OAuth2 return URLs	Read	workload-identity*		
			workload-identity-directory*		
InvokeAgentRuntime	Grants permission to invoke an agent runtime endpoint	Write	runtime*		
			runtime-endpoint*		
InvokeAgentRuntimeCommand	Grants permission to invoke commands on an agent runtime endpoint	Write	runtime*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			runtime-endpoint*		
InvokeAgentRuntimeForUser	Grants permission to invoke an agent runtime endpoint with X-Amzn-Bedrock-AgentCore-Runtime-User-Id header	Write	runtime*		
			runtime-endpoint*		
InvokeAgentRuntimeWithWebSocketStream	Grants permission to invoke an agent runtime endpoint with WebSocket stream	Write	runtime*		
			runtime-endpoint*		
InvokeAgentRuntimeWithWebSocketStreamForUser	Grants permission to invoke an agent runtime endpoint with WebSocket stream and with X-Amzn-Bedrock-AgentCore-Runtime-User-Id header	Write	runtime*		
			runtime-endpoint*		
InvokeCodeInterpreter	Grants permission to invoke a code interpreter session	Write	code-interpreter*		
			code-interpreter-custom*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvokeGateway [permission only]	Grants permission to invoke a gateway	Permissions management	gateway*		
ListActors	Grants permission to list Actors	List	memory*		
ListAgentRuntimeEndpoints	Grants permission to list agent runtime endpoints	List			
ListAgentRuntimeVersions	Grants permission to list agent runtime versions	List			
ListAgentRuntimes	Grants permission to list agent runtimes	List			
ListApiKeyCredentialProviders	Grants permission to list all API Key Credential Providers in the Token Vault	Read	apikeycredentialprovider*		
			token-vault*		
ListBrowserProfiles	Grants permission to list browser profiles	List			
ListBrowserSessions	Grants permission to list browser sessions	List			
ListBrowsers	Grants permission to list browsers	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCodeInterpreterSessions	Grants permission to list code interpreter sessions	List	code-interpreter*		
			code-interpreter-custom*		
ListCodeInterpreters	Grants permission to list code interpreters	List			
ListEvaluators	Grants permission to list evaluators	List			
ListEvents	Grants permission to list events	List	memory*		
				bedrock-agentcore:sessionId bedrock-agentcore:actorId	
ListGatewayTargets	Grants permission to list existing gateway targets	List	gateway*		
ListGateways	Grants permission to list existing gateways	List			
ListMemories	Grants permission to list memory resources	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMemoryExtractionJobs	Grants permission to list extraction jobs for this memory	List	memory*		
ListMemoryRecords	Grants permission to list memory records	List	memory*		
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
ListOauth2CredentialProviders	Grants permission to list all OAuth2 Credential Providers in the Token Vault	Read	oauth2credentialprovider*		
			token-vault*		
ListOnlineEvaluationConfigs	Grants permission to list online evaluation configurations	List			
ListPolicies	Grants permission to list policies within a policy engine	List	policy-engine*		
ListPolicyEngines	Grants permission to list policy engines	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPolicyGenerationAssets	Grants permission to list generated policy assets from a generation request	List	policy-engine*		
			policy-generation*		
ListPolicyGenerations	Grants permission to list policy generation requests	List	policy-engine*		
ListSessions	Grants permission to list sessions	List	memory*		
				bedrock-agentcore:actorId	
ListTagsForResource	Grants permission to list tags for a Bedrock-AgentCore resource	List	apikeycredentialprovider		
			browser-custom		
			browser-profile		
			code-interpreter-custom		
			evaluator		
			gateway		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			memory		
			oauth2credentialprovider		
			online-evaluation-config		
			runtime		
			runtime-endpoint		
			token-vault		
			workload-identity		
			workload-identity-directory		
ListWorkloadIdentities	Grants permission to list all Workload Identities in the caller's AWS account	Read	workload-identity*		
			workload-identity-directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ManageAdminPolicy [permission only]	Grants permission to create or modify wildcard policies that apply to gateway resources	Permissions management			
ManageResourceScopedPolicy [permission only]	Grants permission to create or modify policies that apply to specific gateway resources	Permissions management	gateway*		
PartiallyAuthorizeActions [permission only]	Grants permission to perform partial evaluation of Cedar policies to authorize a caller to list tools they are allowed to call	Permissions management	gateway* policy-engine*		
PutResourcePolicy	Grants permission to create or update the resource-based policy for a Bedrock resource	Write	gateway runtime runtime-endpoint		
RetrieveMemoryRecords	Grants permission to retrieve memory records through sematic query	List	memory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				bedrock-agentcore:namespace bedrock-agentcore:strategyId	
SaveBrowserSessionProfile	Grants permission to save a browser session profile	Write	browser*		
			browser-custom*		
			browser-profile*		
SetTokenVaultCMK	Grants permission to associate a Customer Managed Key (CMK) or a Service Managed Key with a specific TokenVault	Read	token-vault*		
StartBrowserSession	Grants permission to start a new browser session	Write	browser*		
			browser-custom*		
			browser-profile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCodeInterpreterSession	Grants permission to start a new code interpreter session	Write	code-interpreter*		
			code-interpreter-custom*		
StartMemoryExtractionJob	Grants permission to start memory extraction job	Write	memory*		
				bedrock-agentcore:strategyId bedrock-agentcore:sessionId bedrock-agentcore:actorId	
StartPolicyGeneration	Grants permission to start an AI-powered policy generation request	Write	policy-engine*		
StopBrowserSession	Grants permission to stop a browser session	Write	browser*		
			browser-custom*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopCodeInterpreterSession	Grants permission to stop a code interpreter session	Write	code-interpreter*		
			code-interpreter-custom*		
StopRuntimeSession	Grants permission to stop a runtime session	Write	runtime*		
			runtime-endpoint*		
SynchronizeGatewayTargets [permission only]	Grants permission to enable search on gateways	Permissions management	gateway*		
TagResource	Grants permission to Tag a Bedrock-AgentCore resource	Tagging	apikeycredentialprovider		
			browser-custom		
			browser-profile		
			code-interpreter-custom		
			evaluator		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			gateway		
			memory		
			oauth2credentialprovider		
			online-evaluation-config		
			runtime		
			runtime-endpoint		
			token-vault		
			workload-identity		
			workload-identity-directory		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to Untag a Bedrock-AgentCore resource	Tagging	apikeycredentialprovider		
			browser-custom		
			browser-profile		
			code-interpreter-custom		
			evaluator		
			gateway		
			memory		
			oauth2credentialprovider		
			online-evaluation-config		
			runtime		
			runtime-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			token-vault		
			workload-identity		
			workload-identity-directory		
				aws:TagKeys	
UpdateAgentRuntime	Grants permission to update an agent runtime	Write	runtime*		iam:PassRole
				bedrock-agentcore:subnets bedrock-agentcore:securityGroups	
UpdateAgentRuntimeEndpoint	Grants permission to update an agent runtime endpoint	Write	runtime*		
			runtime-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApiKeyCredentialProvider	Grants permission to update an existing API Key Credential Provider	Write	apikeycredentialprovider*		
			token-vault*		
UpdateBrowserStream	Grants permission to update the status of browser session stream	Write	browser*		
			browser-custom*		
UpdateEvaluator	Grants permission to update an evaluator	Write	evaluator*		
UpdateGateway	Grants permission to update an existing gateway	Write	gateway*		iam:PassRole
UpdateGatewayTarget	Grants permission to update an existing gateway target	Write	gateway*		
UpdateMemory	Grants permission to update a Memory resource	Write	memory*		iam:PassRole
UpdateOauth2CredentialProvider	Grants permission to update an existing OAuth2 Credential Provider	Write	oauth2credentialprovider*		
			token-vault*		
UpdateOnlineEvaluationConfig	Grants permission to update an online evaluation configuration	Write	online-evaluation-config*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePolicy	Grants permission to update an existing policy	Write	policy*		
			policy-engine*		
UpdatePolicyEngine	Grants permission to update a policy engine	Write	policy-engine*		
UpdateWorkloadIdentity	Grants permission to update the metadata of an existing Workload Identity	Write	workload-identity*		
			workload-identity-directory*		

Resource types defined by Amazon Bedrock Agentcore

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
evaluator	`arn:${Partition}:bedrock-agentcore:${Region}:${Account}:evaluator/${EvaluatorId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
online-evaluation-config	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:online-evaluation-config/${OnlineEvaluationConfigId}	aws:ResourceTag/${TagKey}
memory	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:memory/${MemoryId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
workload-identity	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}/workload-identity/${WorkloadIdentityName}	aws:ResourceTag/${TagKey}
oauth2credentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/oauth2credentialprovider/${Name}	aws:ResourceTag/${TagKey}
apikeycredentialprovider	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}/apikeycredentialprovider/${Name}	aws:ResourceTag/${TagKey}
runtime	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}	aws:ResourceTag/${TagKey}
runtime-endpoint	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:runtime/${RuntimeId}/runtime-endpoint/${Name}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
code-interpreter-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:code-interpreter-custom/${CodeInterpreterId}	aws:ResourceTag/${TagKey}
code-interpreter	arn:${Partition}:bedrock-agentcore:${Region}:aws:code-interpreter/${CodeInterpreterId}	
browser-custom	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:browser-custom/${BrowserId}	aws:ResourceTag/${TagKey}
browser	arn:${Partition}:bedrock-agentcore:${Region}:aws:browser/${BrowserId}	
browser-profile	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:browser-profile/${BrowserProfileId}	aws:ResourceTag/${TagKey}
workload-identity-directory	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:workload-identity-directory/${DirectoryId}	aws:ResourceTag/${TagKey}
token-vault	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:token-vault/${TokenVaultId}	aws:ResourceTag/${TagKey}
policy-engine	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:policy-engine/${PolicyEngineId}	
policy	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:policy-engine/${PolicyEngineId}/policy/${PolicyId}	

Resource types	ARN	Condition keys
policy-generation	arn:${Partition}:bedrock-agentcore:${Region}:${Account}:policy-engine/${PolicyEngineId}/policy-generation/${PolicyGenerationId}	

Condition keys for Amazon Bedrock Agentcore

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

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

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by creating requests based on the allowed set of values for each of the mandatory tags	String
aws:ResourceTag/${TagKey}	Filters access by having actions based on the tag value associated with the resource	String
aws:TagKeys	Filters access by creating requests based on the presence of mandatory tags in the request	ArrayOfString
bedrock-agentcore:GatewayAuthorizerType	Filters access by the authorizerType attribute on a Gateway	String
bedrock-agentcore:	Filters access by the audience claim (aud) in the JWT passed in the request	ArrayOfString

Condition keys	Description	Type
InboundJwtClaim/aud		
bedrock-agentcore:InboundJwtClaim/client_id	Filters access by the client_id claim in the JWT passed in the request	String
bedrock-agentcore:InboundJwtClaim/iss	Filters access by the issuer (iss) claim present in the JWT passed in the request	String
bedrock-agentcore:InboundJwtClaim/scope	Filters access by the scope claim in the JWT passed in the request	ArrayOfString
bedrock-agentcore:InboundJwtClaim/sub	Filters access by the subject claim (sub) in the JWT passed in the request	String
bedrock-agentcore:KmsKeyArn	Filters access by KMS Key arn provided	String
bedrock-agentcore:actorId	Filters access by Actor Id	String
bedrock-agentcore:namespace	Filters access by namespace	String
bedrock-agentcore:securityGroups	Filters access by the ID of security groups configured for the AgentCore runtime	ArrayOfString

Condition keys	Description	Type
bedrock-agentcore:sessionId	Filters access by Session Id	String
bedrock-agentcore:strategyId	Filters access by Memory Strategy Id	String
bedrock-agentcore:subnets	Filters access by the ID of subnets configured for the AgentCore runtime	ArrayOfString
bedrock-agentcore:userid	Filters access by the static user ID value passed in the request	String

Actions, resources, and condition keys for Amazon Bedrock Powered by AWS Mantle

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

References:

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

Topics

- Actions defined by Amazon Bedrock Powered by AWS Mantle
- Resource types defined by Amazon Bedrock Powered by AWS Mantle
- Condition keys for Amazon Bedrock Powered by AWS Mantle

Actions defined by Amazon Bedrock Powered by AWS Mantle

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ArchiveProject	Grants permission to archive a specific project	Write	project*	aws:ResourceTag/${TagKey}	
CallWithBearerToken [permission only]	Grants permission to make API calls using bearer token authentication	List		bedrock-mantle:BearerTokenType	
CancelFineTuningJob	Grants permission to cancel an in-progress fine tuning job	Write	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:FineTuningJob	
CancelInference	Grants permission to cancel an in-progress inference request	Write	project*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFile	Grants permission to create a file in a project	Write	project*	aws:ResourceTag/${TagKey}	
CreateFineTuningJob	Grants permission to create a fine tuning job	Write	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:Model bedrock-mantle:Files	
CreateInference	Grants permission to create a chat completion inference request	Write	project*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				bedrock-mantle:ServiceTier bedrock-mantle:Model	
CreateProject	Grants permission to create a project	Write	project*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFile	Grants permission to delete a specific file	Write	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:Files	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInference	Grants permission to delete a specific inference request	Write	project*	aws:ResourceTag/${TagKey}	
GetFile	Grants permission to retrieve information about a specific file	Read	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:Files	
GetFineTuningJob	Grants permission to retrieve details of a specific fine tuning job	Read	project*	aws:ResourceTag/${TagKey}	
				bedrock-mantle:FineTuningJob	
GetInference	Grants permission to retrieve details of a specific inference request	Read	project*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetModel	Grants permission to retrieve information about a specific model	Read	project*	aws:ResourceTag/${TagKey}	
GetProject	Grants permission to retrieve details of a specific project	Read	project*	aws:ResourceTag/${TagKey}	
ListFiles	Grants permission to list all available files in a project	List	project*	aws:ResourceTag/${TagKey}	
ListFineTuningJobs	Grants permission to list all available fine tuning jobs in a project	List	project*	aws:ResourceTag/${TagKey}	
ListModels	Grants permission to list all available models in a project	List	project*	aws:ResourceTag/${TagKey}	
ListProjects	Grants permission to list projects	List	project*		
ListTagsForResource	Grants permission to list tags for a resource	Read	project	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging	project	aws:ResourceTag/${TagKey}	
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	project	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateProject	Grants permission to update a specific project	Write	project*	aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Bedrock Powered by AWS Mantle

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:${Partition}:bedrock-mantle:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Bedrock Powered by AWS Mantle

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

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

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
bedrock-mantle:BearerTokenType	Filters access by the Short-term or Long-term bearer tokens	String
bedrock-mantle:Files	Filters access by the specified file identifiers	ArrayOfString

Condition keys	Description	Type
bedrock-mantle:FineTuningJob	Filters access by the specified fine-tuning job identifier	String
bedrock-mantle:Model	Filters access by the specified Model	String
bedrock-mantle:ServiceTier	Filters access by the specified ServiceTier	String

Actions, resources, and condition keys for AWS Billing

AWS 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 AWS Billing
- Resource types defined by AWS Billing
- Condition keys for AWS Billing

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateSourceViews	Grants permission to associate source views to a billing view	Write	billingview*		billing:UseSourceView iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
CreateBillingView	Grants permission to create a billing view	Write	billingview*		billing:UseSourceView iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBillingView	Grants permission to delete a billing view	Write	billingview*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
DeleteResourcePolicy [permission only]	Grants permission to delete a billing view resource policy	Permissions management	billingview*		
				aws:ResourceTag/${TagKey}	
DisassociateSourceViews	Grants permission to disassociate source views from a billing view	Write	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData [permission only]	Grants permission to perform queries on billing information	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetBillingDetails [permission only]	Grants permission to view detailed line item billing information	Read	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBillingNotifications [permission only]	Grants permission to view notifications sent by AWS 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}	
GetBillingViewData [permission only]	Grants permission to get cost and usage data for a specified billng view	Read	billingview*		
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 AWS 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			
UseSourceView [permission only]	Grants permission to use a billing view as a data source for other billing views	Read			

Resource types defined by AWS 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 AWS Billing

AWS 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 AWS global condition context keys.

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

Actions, resources, and condition keys for AWS Billing and Cost Management Dashboards

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

References:

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

Topics

- Actions defined by AWS Billing and Cost Management Dashboards

- Resource types defined by AWS Billing and Cost Management Dashboards
- Condition keys for AWS Billing and Cost Management Dashboards

Actions defined by AWS Billing and Cost Management Dashboards

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDashboard	Grants permission to create a dashboard	Write			
DeleteDashboard	Grants permission to delete a dashboard	Write			
GetDashboard	Grants permission to get dashboard information	Read			
GetResourcePolicy	Grants permission to get the resource policy for a dashboard	Read			
ListDashboards	Grants permission to list information about all of the dashboards for a user	Read			
ListTagsForResource	Grants permission to list all of the tags for a resource	Read			
TagResource	Grants permission to create a tag for a resource	Tagging		aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag for a resource	Tagging		aws:TagKeys	
UpdateDashboard	Grants permission to update an existing dashboard	Write			

Resource types defined by AWS Billing and Cost Management Dashboards

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

Condition keys for AWS Billing and Cost Management Dashboards

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

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

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

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

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

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

References:

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

Topics

Actions defined by AWS Billing And Cost Management Data Exports

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExport	Grants permission to create an export	Write	table*		

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

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

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

Resource types defined by AWS Billing And Cost Management Data Exports

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

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

Condition keys for AWS Billing And Cost Management Data Exports

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

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

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

Actions, resources, and condition keys for AWS Billing And Cost Management Pricing Calculator

AWS Billing And Cost Management Pricing Calculator (service prefix: `bcm-pricing-calculator`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

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

Topics

Actions defined by AWS Billing And Cost Management Pricing Calculator

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

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBillEstimate	Grants permission to create a new bill estimate. Charge is incurred for successful bill estimates	Write	bill-scenario		
CreateBillScenario	Grants permission to create a new bill scenario	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateBillScenarioCommitmentModification	Grants permission to create new commitments or remove existing commitment from a specified bill scenario	Write	bill-scenario*		
CreateBillScenarioUsageModification	Grants permission to create usage in the specified bill scenario	Write	bill-scenario*		
CreateWorkloadEstimate	Grants permission to create a new Workload estimate	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkloadEstimateUsage	Grants permission to create usage in the specified workload estimate	Write	workload-estimate*		
DeleteBillEstimate	Grants permission to delete bill estimate	Write	bill-estimate*		
DeleteBillScenario	Grants permission to delete a bill scenario	Write	bill-scenario*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBillScenarioCommitmentModification	Grants permission to delete newly added commitments from the specified bill scenario	Write	bill-scenario*		
DeleteBillScenarioUsageModification	Grants permission to delete newly added usage from the specified bill scenario	Write	bill-scenario*		
DeleteWorkloadEstimate	Grants permission to delete the specified workload estimate	Write	workload-estimate*		
DeleteWorkloadEstimateUsage	Grants permission to delete newly added usage from the specified workload estimate	Write	workload-estimate*		
GetBillEstimate	Grants permission to retrieve details of a bill estimate including estimated cost	Read	bill-estimate*		
GetBillScenario	Grants permission to retrieve information associated with a bill scenario	Read	bill-scenario*		
GetPreferences	Grants permission to retrieve applicable rate type preferences for the account	Read			
GetWorkloadEstimate	Grants permission to retrieve information associated with a workload estimate	Read	workload-estimate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBillEstimateCommitments	Grants permission to list commitments associated with the specified bill estimate	List	bill-estimate*		
ListBillEstimateInputCommitmentModifications	Grants permission to list added or removed commitments for a specified bill estimate	List	bill-estimate*		
ListBillEstimateInputUsageModifications	Grants permission to list added or modified usage for a specified bill estimate	List	bill-estimate*		
ListBillEstimateLineItems	Grants permission to list result line items for a specified bill estimate	List	bill-estimate*		
ListBillEstimates	Grants permission to list bill estimates	List			
ListBillScenarioCommitmentModifications	Grants permission to list commitments included in a bill scenario	List	bill-scenario*		
ListBillScenarioUsageModifications	Grants permission to list usage lines of a specified bill scenario	List	bill-scenario*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBillScenarios	Grants permission to list bill scenarios	List			
ListTagsForResource	Grants permission to return a list of tags for a resource	Tagging			
ListWorkloadEstimateUsage	Grants permission to list usage lines for the specified workload estimate	List	workload-estimate*		
ListWorkloadEstimates	Grants permission to list workload estimates	List			
TagResource	Grants permission to add a tag to a resource	Tagging	bill-scenario	aws:ResourceTag/${TagKey}	
			workload-estimate	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove a tag from a resource	Tagging	bill-scenario	aws:ResourceTag/${TagKey}	
			workload-estimate	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateBillEstimate	Grants permission to update bill estimate name and expiration date time	Write	bill-estimate*		
UpdateBillScenario	Grants permission to update name and expiration date time of the specified bill scenario	Write	bill-scenario*		
UpdateBillScenarioCommitmentModification	Grants permission to update commitment group of commitments in the specified bill scenario	Write	bill-scenario*		
UpdateBillScenarioUsageModification	Grants permission to update usage amount, usage hour, and usage group in the specified bill scenario	Write	bill-scenario*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePreferences	Grants permission to update rate type preferences for the account	Write			
UpdateWorkloadEstimate	Grants permission to update name and expiration date time of the specified workload estimate	Write	workload-estimate*		
UpdateWorkloadEstimateUsage	Grants permission to update usage amount and usage group in the specified workload estimate based on the usage id	Write	workload-estimate*		

Resource types defined by AWS Billing And Cost Management Pricing Calculator

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
bill-estimate	`arn:${Partition}:bcm-pricing-calculator::${Account}:bill-estimate/${BillEstimateId}`	

Resource types	ARN	Condition keys
bill-scenario	arn:${Partition}:bcm-pricing-calculator::${Account}:bill-scenario/${BillScenarioId}	aws:ResourceTag/${TagKey}
workload-estimate	arn:${Partition}:bcm-pricing-calculator::${Account}:workload-estimate/${WorkloadEstimateId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Billing And Cost Management Pricing Calculator

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

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

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

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

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

References:

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

Topics

Actions defined by AWS Billing And Cost Management Recommended Actions

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecommendedActions	Grants permission to list all recommended actions	List			

Resource types defined by AWS Billing And Cost Management Recommended Actions

AWS Billing And Cost Management Recommended Actions does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Billing And Cost Management Recommended Actions, specify `"Resource": "*"` in your policy.

Condition keys for AWS Billing And Cost Management Recommended Actions

BillingAndCostManagementRecommendedActions has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Billing Conductor

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

References:

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

Topics

Actions defined by AWS Billing Conductor

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAccounts	Grants permission to associate between one and 30 accounts to a billing group	Write	billinggroup*		
AssociatePricingRules	Grants permission to associate pricing rules	Write	pricingplan*		
			pricingrule*		
BatchAssociateResourcesToCustomLineItem	Grants permission to batch associate resources to a percentage custom line item	Write	customlineitem*		
BatchDisassociateResourcesFromCustomLineItem	Grants permission to batch disassociate resources from a percentage custom line item	Write	customlineitem*		
CreateBillingGroup	Grants permission to create a billing group	Write	pricingplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomLineItem	Grants permission to create a custom line item	Write	billinggroup*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingPlan	Grants permission to create a pricing plan	Write	pricingrule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePricingRule	Grants permission to create a pricing rule	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteBillingGroup	Grants permission to delete a billing group	Write	billinggroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomLineItem	Grants permission to delete a custom line item	Write	customlineitem*		
DeletePricingPlan	Grants permission to delete a pricing plan	Write	pricingplan*		
DeletePricingRule	Grants permission to delete a pricing rule	Write	pricingrule*		
DisassociateAccounts	Grants permission to detach between one and 30 accounts from a billing group	Write	billinggroup*		
DisassociatePricingRules	Grants permission to disassociate pricing rules	Write	pricingplan*		
			pricingrule*		
GetBillingGroupCostReport	Grants permission to view the billing group cost report for the specified billing group	Read	billinggroup*		
ListAccountAssociations	Grants permission to list the linked accounts of the payer account for the given billing period while also providing the billing group the linked accounts belong to	List			
ListBillingGroupCostReports	Grants permission to view the billing group cost report	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBillingGroups	Grants permission to view the details of billing groups	Read			
ListCustomLineItemVersions	Grants permission to view custom line item versions	Read	customlineitem*		
ListCustomLineItems	Grants permission to view custom line item details	Read			
ListPricingPlans	Grants permission to view the pricing plans details	Read			
ListPricingPlansAssociatedWithPricingRule	Grants permission to list pricing plans associated with a pricing rule	List	pricingrule*		
ListPricingRules	Grants permission to view pricing rules details	Read			
ListPricingRulesAssociatedToPricingPlan	Grants permission to list pricing rules associated to a pricing plan	List	pricingplan*		
ListResourcesAssociatedToCustomLineItem	Grants permission to list resources associated to a percentage custom line item	List	customlineitem*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags of a resource	Read	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Grants permission to tag a resource	Tagging	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	billinggroup		
			customlineitem		
			pricingplan		
			pricingrule		
				aws:TagKeys	
UpdateBillingGroup	Grants permission to update a billing group	Write	billinggroup*		
UpdateCustomLineItem	Grants permission to update a custom line item	Write	customlineitem*		
UpdatePricingPlan	Grants permission to update a pricing plan	Write	pricingplan*		
UpdatePricingRule	Grants permission to update a pricing rule	Write	pricingrule*		

Resource types defined by AWS Billing Conductor

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
billinggroup	`arn:${Partition}:billingconductor::${Account}:billinggroup/${BillingGroupId}`	aws:ResourceTag/${TagKey}
pricingplan	`arn:${Partition}:billingconductor::${Account}:pricingplan/${PricingPlanId}`	aws:ResourceTag/${TagKey}
pricingrule	`arn:${Partition}:billingconductor::${Account}:pricingrule/${PricingRuleId}`	aws:ResourceTag/${TagKey}
customlineitem	`arn:${Partition}:billingconductor::${Account}:customlineitem/${CustomLineItemId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Billing Conductor

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

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

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

Actions, resources, and condition keys for AWS Billing Console

AWS 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 AWS Billing Console
- Resource types defined by AWS Billing Console
- Condition keys for AWS Billing Console

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS usage reports	Read			

Resource types defined by AWS Billing Console

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

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for Amazon Braket

Amazon Braket (service prefix: `braket`) 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 Braket

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

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

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

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

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptUserAgreement [permission only]	Grants permission to accept the Amazon Braket user agreement	Write			
CancelJob	Grants permission to cancel a job	Write	job*		
CancelQuantumTask	Grants permission to cancel a quantum task	Write	quantum-task*		
CreateJob	Grants permission to create a job	Write		aws:RequestTag/${TagKey} aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateQuantumTask	Grants permission to create a quantum task	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateSpendingLimit	Grants permission to create a spending limit	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSpendingLimit	Grants permission to delete a spending limit	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
GetDevice	Grants permission to retrieve information about the devices available in Amazon Braket	Read			
GetJob	Grants permission to retrieve jobs	Read	job*		
GetQuantumTask	Grants permission to retrieve quantum tasks	Read	quantum-task*		
GetServiceLinkedRoleStatus [permission only]	Grants permission to check if the Amazon Braket service linked role has been created	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserAgreementStatus [permission only]	Grants permission to check if the account has accepted the Amazon Braket user agreement	Read			
ListTagsForResource	Grants permission to listing the tags that have been applied to the quantum task resource or the job	Read	job		
			quantum-task		
			spending-limit		
SearchDevices	Grants permission to search for devices available in Amazon Braket	Read			
SearchJobs	Grants permission to search for jobs	Read			
SearchQuantumTasks	Grants permission to search for quantum tasks	Read			
SearchSpendingLimits	Grants permission to search for spending limit	Read			
TagResource	Grants permission to add one or more tags to a quantum task or a hybrid job	Tagging	job		
			quantum-task		
			spending-limit		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a quantum task resource or a job. A tag consists of a key-value pair	Tagging	job		
			quantum-task		
			spending-limit		
				aws:TagKeys	
UpdateSpendingLimit	Grants permission to update a spending limit	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Resource types defined by Amazon Braket

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
quantum-task	`arn:${Partition}:braket:${Region}:${Account}:quantum-task/${RandomId}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:braket:${Region}:${Account}:job/${JobName}`	aws:ResourceTag/${TagKey}
spending-limit	`arn:${Partition}:braket:${Region}:${Account}:spending-limit/${RandomId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Braket

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

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

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

Condition keys	Description	Type
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Budget Service

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

References:

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

Topics

Actions defined by AWS Budget Service

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

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBudgetAction	Grants permission to configure a response that executes once your budget exceeds a specific budget 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}	
DeleteBudgetAction	Grants permission to delete an action that is associated with a specific budget	Write	budgetAction*		
DescribeBudgetAction	Grants permission to retrieve the details of a specific budget action associated with a budget	Read	budgetAction*		
DescribeBudgetActionHistories	Grants permission to retrieve a historical view of the budget actions statuses associated with a particular budget action. These status include statues such as 'Standby', 'Pending' and 'Executed'	Read	budgetAction*		

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

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

Resource types defined by AWS Budget Service

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

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

Condition keys for AWS Budget Service

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

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

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

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

Actions, resources, and condition keys for AWS BugBust

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

References:

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

Topics

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

Actions defined by AWS BugBust

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEvent [permission only]	Grants permission to create a BugBust event	Write		aws:TagKeys	iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
EvaluateProfilingGroups [permission only]	Grants permission to evaluate checked-in profiling groups	Write	Event*		
				aws:ResourceTag/${TagKey}	
GetEvent [permission only]	Grants permission to view customer details about an event	Read	Event*		
				aws:ResourceTag/${TagKey}	
GetJoinEventStatus [permission only]	Grants permission to view the status of a BugBust player's attempt to join a BugBust event	Read	Event*		
				aws:ResourceTag/${TagKey}	
JoinEvent [permission only]	Grants permission to join an event	Write	Event*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBugs [permission only]	Grants permission to view the bugs that were imported into an event for players to work on	Read	Event*		codeguru-reviewer: DescribeCodeReview codeguru-reviewer: ListRecommendations
				aws:ResourceTag/${TagKey}	
ListEventParticipants [permission only]	Grants permission to view the participants of an event	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListEventScores [permission only]	Grants permission to view the scores of an event's players	Read	Event*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEvents [permission only]	Grants permission to List BugBust events	List		aws:ResourceTag/${TagKey}	
ListProfilingGroups [permission only]	Grants permission to view the profiling groups that were imported into an event for players to work on	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListPullRequests [permission only]	Grants permission to view the pull requests used by players to submit fixes to their claimed bugs in an event	Read	Event*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [permission only]	Grants permission to lists tag for a Bugbust resource	Read	Event*		
				aws:ResourceTag/${TagKey}	
TagResource [permission only]	Grants permission to tag a Bugbust resource	Tagging	Event*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [permission only]	Grants permission to untag a Bugbust resource	Tagging	Event*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEvent [permission only]	Grants permission to update a BugBust event	Write	Event*		codeguru-profiler:DescribeProfilingGroup codeguru-profiler:ListProfilingGroups codeguru-reviewer:DescribeCodeReview codeguru-reviewer:ListCodeReviews codeguru-reviewer:ListRecommendations codeguru-reviewer:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					codeguru-reviewer:UnTagResource
				aws:ResourceTag/${TagKey}	
UpdateWorkItem [permission only]	Grants permission to update a work item as claimed or unclaimed (bug or profiling group)	Write	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	
UpdateWorkItemAdmin [permission only]	Grants permission to update an event's work item (bug or profiling group)	Write	Event*		codeguru-reviewer:ListRecommendations
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS BugBust

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:${Partition}:bugbust:${Region}:${Account}:events/${EventId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS BugBust

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

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

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

Actions, resources, and condition keys for AWS Certificate Manager

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

References:

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

Topics

Actions defined by AWS Certificate Manager

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

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

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

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

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

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

Note

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToCertificate	Grants permission to add one or more tags to a certificate	Tagging	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

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

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

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

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

Resource types defined by AWS Certificate Manager

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

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

Condition keys for AWS Certificate Manager

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

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

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

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

Actions, resources, and condition keys for AWS Chatbot

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

References:

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

Topics

Actions defined by AWS Chatbot

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateToConfiguration	Grants permission to associate a resource with a configuration	Write	ChatbotConfiguration*		
			custom-action*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
CreateChimeWebhookConfiguration	Grants permission to create an AWS Chatbot Chime Webhook Configuration	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomAction	Grants permission to create a custom action	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMicrosoftTeamsChannelConfiguration	Grants permission to create an AWS Chatbot Microsoft Teams Channel Configuration	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSlackChannelConfiguration	Grants permission to create an AWS Chatbot Slack Channel Configuration	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteChimeWebhookConfiguration	Grants permission to delete an AWS Chatbot Chime Webhook Configuration	Write	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteCustomAction	Grants permission to delete a custom action	Write	custom-action*		
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsChannelConfiguration	Grants permission to delete an AWS Chatbot Microsoft Teams Channel Configuration	Write	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteMicrosoftTeamsConfiguredTeam	Grants permission to delete the Microsoft Teams configured with AWS Chatbot in an AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMicrosoftTeamsUserIdentity	Grants permission to delete an AWS Chatbot Microsoft Teams User Identity	Write			
DeleteSlackChannelConfiguration	Grants permission to delete an AWS Chatbot Slack Channel Configuration	Write	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteSlackUserIdentity	Grants permission to delete an AWS Chatbot Slack User Identity	Write			
DeleteSlackWorkspaceAuthorization	Grants permission to delete the Slack workspace authorization with AWS Chatbot, associated with an AWS account	Write			
DescribeChimeWebhookConfigurations	Grants permission to list all AWS Chatbot Chime Webhook Configurations in an AWS Account	Read			
DescribeSlackChannelConfigurations	Grants permission to list all AWS Chatbot Slack Channel Configurations in an AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSlackChannels	Grants permission to list all public Slack channels in the Slack workspace connected to the AWS Account onboarded with AWS Chatbot service	Read			
DescribeSlackUserIdentities	Grants permission to describe AWS Chatbot Slack User Identities	Read			
DescribeSlackWorkspaces	Grants permission to list all authorized Slack workspaces connected to the AWS Account onboarded with AWS Chatbot service	Read			
DisassociateFromConfiguration	Grants permission to disassociate a resource from a configuration	Write	ChatbotConfiguration*		
			custom-action*		
				aws:ResourceTag/${TagKey}	
GetAccountPreferences	Grants permission to retrieve AWS Chatbot account preferences	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCustomAction	Grants permission to get a custom action	Read	custom-action*		
				aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsChannelConfigurations	Grants permission to get a single AWS Chatbot Microsoft Teams Channel Configurations in an AWS account	Read		aws:ResourceTag/${TagKey}	
GetMicrosoftTeamsOauthParameters	Grants permission to generate OAuth parameters to request Microsoft Teams OAuth code to be used by the AWS Chatbot service	Read			
GetSlackOauthParameters	Grants permission to generate OAuth parameters to request Slack OAuth code to be used by the AWS Chatbot service	Read			
ListAssociations	Grants permission to list resources associated with a configuration	Read	ChatbotConfiguration*		
ListCustomActions	Grants permission to list custom actions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMicrosoftTeamsChannelConfigurations	Grants permission to list all AWS Chatbot Microsoft Teams Channel Configurations in an AWS account	Read			
ListMicrosoftTeamsConfiguredTeams	Grants permission to list all Microsoft Teams connected to the AWS Account onboarded with AWS Chatbot service	Read			
ListMicrosoftTeamsUserIdentities	Grants permission to describe AWS Chatbot Microsoft Teams User Identities	Read			
ListTagsForResource	Grants permission to List all tags associated with the AWS Chatbot Channel Configuration	Read			
RedeemMicrosoftTeamsOauthCode	Grants permission to redeem previously generated parameters with Microsoft APIs, to acquire OAuth tokens to be used by the AWS Chatbot service	Write			
RedeemSlackOauthCode	Grants permission to redeem previously generated parameters with Slack API, to acquire OAuth tokens to be used by the AWS Chatbot service	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to create tags on AWS Chatbot Channel Configuration	Tagging	ChatbotConfiguration		
			custom-action		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags on AWS Chatbot Channel Configuration	Tagging	ChatbotConfiguration		
			custom-action		
				aws:TagKeys	
UpdateAccountPreferences	Grants permission to update AWS Chatbot account preferences	Write			
UpdateChimeWebhookConfiguration	Grants permission to update an AWS Chatbot Chime Webhook Configuration	Write	ChatbotConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateCustomAction	Grants permission to update a custom action	Write	custom-action*		
				aws:ResourceTag/${TagKey}	
UpdateMicrosoftTeamsChannelConfiguration	Grants permission to update an AWS Chatbot Microsoft Teams Channel Configuration	Write	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateSlackChannelConfiguration	Grants permission to update an AWS Chatbot Slack Channel Configuration	Write	ChatbotConfiguration*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS Chatbot

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
ChatbotConfiguration	`arn:${Partition}:chatbot::${Account}:chat-configuration/${ConfigurationType}/${ChatbotConfigurationName}`	aws:ResourceTag/${TagKey}
custom-action	`arn:${Partition}:chatbot::${Account}:custom-action/${ActionName}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Chatbot

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

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

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

Actions, resources, and condition keys for Amazon Chime

Amazon Chime (service prefix: `chime`) 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 Chime

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDelegate	Grants permission to accept the delegate invitation to share management of an Amazon Chime account with another AWS Account	Write			
ActivateUsers	Grants permission to activate users in an Amazon Chime Enterprise account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddDomain	Grants permission to add a domain to your Amazon Chime account	Write			
AddOrUpdateGroups	Grants permission to add new or update existing Active Directory or Okta user groups associated with your Amazon Chime Enterprise account	Write			
AssociateChannelFlow	Grants permission to associate a flow with a channel	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		
AssociatePhoneNumberWithUser	Grants permission to associate a phone number with an Amazon Chime user	Write			
AssociatePhoneNumbersWithVoiceConnector	Grants permission to associate multiple phone numbers with an Amazon Chime Voice Connector	Write	voice-connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociatePhoneNumbersWithVoiceConnectorGroup	Grants permission to associate multiple phone numbers with an Amazon Chime Voice Connector Group	Write			
AssociateSigninDelegateGroupsWithAccount	Grants permission to associate the specified sign-in delegate groups with the specified Amazon Chime account	Write			
AssociateVoiceConnectorConnect [permission only]	Grants permission to associate the specified Amazon Connect instance with an Amazon Chime Voice Connector	Write			
AuthorizeDirectory	Grants permission to authorize an Active Directory for your Amazon Chime Enterprise account	Write			
BatchCreateAttendee	Grants permission to create new attendees for an active Amazon Chime SDK meeting	Write	meeting*		
BatchCreateChannelMembership	Grants permission to add multiple users and bots to a channel	Write	app-instance-bot* app-instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			channel*		
BatchCreateRoomMembership	Grants permission to batch add room members	Write			
BatchDeletePhoneNumber	Grants permission to move up to 50 phone numbers to the deletion queue	Write			
BatchSuspendUser	Grants permission to suspend up to 50 users from a Team or EnterpriseLWA Amazon Chime account	Write			
BatchUnsuspendUser	Grants permission to remove the suspension from up to 50 previously suspended users for the specified Amazon Chime EnterpriseLWA account	Write			
BatchUpdateAttendeeCapabilitiesExcept	Grants permission to update AttendeeCapabilities except the capabilities listed in an ExcludedAttendeeIds table	Write	meeting*		
BatchUpdatePhoneNumber	Grants permission to update phone number details within the UpdatePhoneNumberRequestItem object for up to 50 phone numbers	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateUser	Grants permission to update user details within the UpdateUserRequestItem object for up to 20 users for the specified Amazon Chime account	Write			
ChannelFlowCallback	Grants permission to callback for a message on a channel	Write	channel*		
Connect	Grants permission to establish a web socket connection for app instance user to the messaging session endpoint	Write	app-instance-user*		
ConnectDirectory	Grants permission to connect an Active Directory to your Amazon Chime Enterprise account	Write			ds:ConnectDirectory
CreateAccount	Grants permission to create an Amazon Chime account under the administrator's AWS account	Write			
CreateApiKey	Grants permission to create a new SCIM access key for your Amazon Chime account and Okta configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppInstance	Grants permission to create an app instance in the AWS account (tag-based access controls are only supported on identity-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceAdmin	Grants permission to promote a user or bot to an AppInstanceAdmin	Write	app-instance*		
			app-instance-bot*		
			app-instance-user*		
CreateAppInstanceBot	Grants permission to create a bot within an AppInstance (tag-based access controls are only supported on identity-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAppInstanceUser	Grants permission to create a user within an AppInstance (tag-based access controls are only supported on identity-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAttendee	Grants permission to create a new attendee for an active Amazon Chime SDK meeting	Write	meeting*		
CreateBot	Grants permission to create a bot for an Amazon Chime Enterprise account	Write			
CreateCDRBucket	Grants permission to create a new Call Detail Record S3 bucket	Write			s3:CreateBucket s3:ListAllMyBuckets
CreateChannel	Grants permission to create a channel for an app instance in the AWS account (tag-based access controls are only supported on messaging-chime.<region>.amazonaws.com endpoints)	Write	app-instance-bot*		
			app-instance-user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelBan	Grants permission to ban a user or bot from a channel	Write	app-instance-bot*		
			app-instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			channel*		
CreateChannelFlow	Grants permission to create a channel flow for an app instance in the AWS account (tag-based access controls are only supported on messaging-chime.<region>.amazonaws.com endpoints)	Write	app-instance*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateChannelMembership	Grants permission to add a user or bot to a channel	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
CreateChannelModerator	Grants permission to create a channel moderator	Write	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnectAnalyticsConnector [permission only]	Grants permission to create an Amazon Connect Analytics Connector in the AWS account (tag-based access controls are only supported on voice-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateConnectCallTransferConnector [permission only]	Grants permission to create an Amazon Connect Call Transfer Connector in the AWS account (tag-based access controls are only supported on voice-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateVoiceConnector
CreateMediaCapturePipeline	Grants permission to create a media capture pipeline (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy
CreateMediaConcatenationPipeline	Grants permission to create a media concatenation pipeline (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	s3:GetBucketPolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMediaInsightsPipeline	Grants permission to create a media insights pipeline (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write	media-insights-pipeline-configuration*		chime:TagResource kinesisvideo:DescribeStream
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMediaInsightsPipelineConfiguration	Grants permission to create a media insights pipeline configuration (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource iam:PassRole kinesis:DescribeStream s3:ListBucket

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMediaLiveConnectorPipeline	Grants permission to create a media live connector pipeline (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMediaPipelineKinesisVideoStreamPool	Grants permission to create kinesis video stream pool (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	kinesis:DescribeStream kinesisvideo:CreateStream kinesisvideo:GetDataEndpoint kinesisvideo:ListStreams

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMediaStreamPipeline	Grants permission to create a media stream pipeline (tag-based access controls are only supported on media-pipelines-chime.<region>.amazonaws.com endpoints)	Write	media-pipeline-kinesis-video-stream-pool*		kinesisvideo:DescribeStream kinesisvideo:GetDataEndpoint kinesisvideo:PutMedia
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMeeting	Grants permission to create a new meeting in the specified media Region, with no initial attendees (tag-based access controls are only supported on meetings-chime.<region>.amazonaws.com endpoints)	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMeetingDialOut	Grants permission to call a phone number to join the specified Amazon Chime SDK meeting	Write	meeting*		
CreateMeetingWithAttendees	Grants permission to create a new meeting in the specified media Region, with a set of attendees (tag-based access controls are only supported on meetings-chime.<region>.amazonaws.com endpoints)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePhoneNumberOrder	Grants permission to create a phone number order with the Carriers	Write			
CreateProxySession	Grants permission to create a proxy session for the specified Amazon Chime Voice Connector	Write	voice-connector*		
CreateRoom	Grants permission to create a room	Write			
CreateRoomMembership	Grants permission to add a room member	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSipMediaApplication	Grants permission to create an Amazon Chime SIP media application in the AWS account (tag-based access controls are only supported on voice-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSipMediaApplicationCall	Grants permission to create outbound call for Amazon Chime SIP media application under the administrator's AWS account	Write	sip-media-application*		
CreateSipRule	Grants permission to create an Amazon Chime SIP rule under the administrator's AWS account	Write	sip-media-application		
CreateUser	Grants permission to create a user under the specified Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVoiceConnector	Grants permission to create a Voice Connector in the AWS account (tag-based access controls are only supported on voice-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	chime:CreateConnectAnalyticsConnector chime:CreateConnectCallTransferConnector
CreateVoiceConnectorGroup	Grants permission to create a Amazon Chime Voice Connector Group under the administrator's AWS account	Write	voice-connector		
CreateVoiceProfile	Grants permission to create a voice profile	Write			
CreateVoiceProfileDomain	Grants permission to create a voice profile domain (tag-based access controls are only supported on voice-chime.<region>.amazonaws.com endpoints)	Write		aws:TagKeys aws:RequestTag/${TagKey}	chime:TagResource kms:CreateGrant kms:DescribeKey
DeleteAccount	Grants permission to delete the specified Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccountOpenIdConfig	Grants permission to delete the OpenIdConfig attributes from your Amazon Chime account	Write			
DeleteApiKey	Grants permission to delete the specified SCIM access key associated with your Amazon Chime account and Okta configuration	Write			
DeleteAppInstance	Grants permission to delete an AppInstance	Write	app-instance*		
DeleteAppInstanceAdmin	Grants permission to demote an AppInstanceAdmin to a user or bot	Write	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DeleteAppInstanceBot	Grants permission to delete an AppInstanceBot	Write	app-instance-bot*		
DeleteAppInstanceStreamingConfigurations	Grants permission to disable data streaming for the app instance	Write	app-instance*		
DeleteAppInstanceUser	Grants permission to delete an AppInstanceUser	Write	app-instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAttendee	Grants permission to delete the specified attendee from an Amazon Chime SDK meeting	Write	meeting*		
DeleteCDRBucket	Grants permission to delete a Call Detail Record S3 bucket from your Amazon Chime account	Write			s3:DeleteBucket
DeleteChannel	Grants permission to delete a channel	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelBan	Grants permission to remove a user or bot from a channel's ban list	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelFlow	Grants permission to delete a channel flow	Write	channel*		
DeleteChannelMembership	Grants permission to remove a member from a channel	Write	app-instance-bot*		
			app-instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			channel*		
DeleteChannelMessage	Grants permission to delete a channel message	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteChannelModerator	Grants permission to delete a channel moderator	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
DeleteDelegate	Grants permission to delete delegated AWS account management from your Amazon Chime account	Write			
DeleteDomain	Grants permission to delete a domain from your Amazon Chime account	Write			
DeleteEventsConfiguration	Grants permission to delete an events configuration for a bot to receive outgoing events	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGroups	Grants permission to delete Active Directory or Okta user groups from your Amazon Chime Enterprise account	Write			
DeleteMediaCapturePipeline	Grants permission to delete a media capture pipeline	Write	media-pipeline*		
DeleteMediaInsightsPipelineConfiguration	Grants permission to delete a media insights pipeline configuration	Write	media-insights-pipeline-configuration*		chime:ListVoiceConnectors
DeleteMediaPipeline	Grants permission to delete a media pipeline	Write	media-pipeline*		
DeleteMediaPipelineKinesisVideoStreamPool	Grants permission to delete kinesis video stream pool	Write	media-pipeline-kinesis-video-stream-pool*		
DeleteMeeting	Grants permission to delete the specified Amazon Chime SDK meeting	Write	meeting*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMessagingStreamingConfigurations	Grants permission to delete the data streaming configurations of an AppInstance	Write	app-instance*		
DeletePhoneNumber	Grants permission to move a phone number to the deletion queue	Write			
DeleteProxySession	Grants permission to delete a proxy session for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteRoom	Grants permission to delete a room	Write			
DeleteRoomMembership	Grants permission to remove a room member	Write			
DeleteSipMediaApplication	Grants permission to delete Amazon Chime SIP media application under the administrator's AWS account	Write	sip-media-application*		
DeleteSipRule	Grants permission to delete Amazon Chime SIP rule under the administrator's AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVoiceConnector	Grants permission to delete the specified Amazon Chime Voice Connector	Write	voice-connector*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries
DeleteVoiceConnectorEmergencyCallingConfiguration	Grants permission to delete emergency calling configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceConnectorExternalSystemsConfiguration	Grants permission to delete the configuration of the external system that is connected with the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceConnectorGroup	Grants permission to delete the specified Amazon Chime Voice Connector Group	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVoiceConnectorOrigination	Grants permission to delete the origination settings for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceConnectorProxy	Grants permission to delete proxy configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceConnectorStreamingConfiguration	Grants permission to delete streaming configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceConnectorTermination	Grants permission to delete the termination settings for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceConnectorTerminationCredentials	Grants permission to delete SIP termination credentials for the specified Amazon Chime Voice Connector	Write	voice-connector*		
DeleteVoiceProfile	Grants permission to delete a voice profile	Write	voice-profile*		
DeleteVoiceProfileDomain	Grants permission to delete a voice profile domain	Write	voice-profile-domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterAppInstanceUserEndpoint	Grants permission to deregister an endpoint for an app instance user	Write	app-instance-user*		
DescribeAppInstance	Grants permission to get the full details of an AppInstance	Read	app-instance*		
DescribeAppInstanceAdmin	Grants permission to get the full details of an AppInstanceAdmin	Read	app-instance*		
			app-instance-bot*		
			app-instance-user*		
DescribeAppInstanceBot	Grants permission to get the full details of an AppInstanceBot	Read	app-instance-bot*		
DescribeAppInstanceUser	Grants permission to get the full details of an AppInstanceUser	Read	app-instance-user*		
DescribeAppInstanceUserEndpoint	Grants permission to describe an endpoint registered for an app instance user	Read	app-instance-user*		
DescribeChannel	Grants permission to get the full details of a channel	Read	app-instance-bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app-instance-user*		
			channel*		
DescribeChannelBan	Grants permission to get the full details of a channel ban	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelFlow	Grants permission to get the full details of a channel flow	Read	channel-flow*		
DescribeChannelMembership	Grants permission to get the full details of a channel membership	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelMembershipForAppInstanceUser	Grants permission to get the details of a channel based on the membership of the specified user or bot	Read	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeChannelModeratedByAppInstanceUser	Grants permission to get the full details of a channel moderated by the specified user or bot	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DescribeChannelModerator	Grants permission to get the full details of a single ChannelModerator	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
DisassociateChannelFlow	Grants permission to disassociate a flow from a channel	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
			channel-flow*		
DisassociatePhoneNumberFromUser	Grants permission to disassociate the primary provisioned number from the specified Amazon Chime user	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociatePhoneNumbersFromVoiceConnector	Grants permission to disassociate multiple phone numbers from the specified Amazon Chime Voice Connector	Write	voice-connector*		
DisassociatePhoneNumbersFromVoiceConnectorGroup	Grants permission to disassociate multiple phone numbers from the specified Amazon Chime Voice Connector Group	Write			
DisassociateSigninDelegateGroupsFromAccount	Grants permission to disassociate the specified sign-in delegate groups from the specified Amazon Chime account	Write			
DisassociateVoiceConnectorConnect [permission only]	Grants permission to disassociate the Amazon Connect instance from the specified Amazon Chime Voice Connector	Write			
DisconnectDirectory	Grants permission to disconnect the Active Directory from your Amazon Chime Enterprise account	Write			
GetAccount	Grants permission to get details for the specified Amazon Chime account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountResource	Grants permission to get details for the account resource associated with your Amazon Chime account	Read			
GetAccountSettings	Grants permission to get account settings for the specified Amazon Chime account ID	Read			
GetAccountWithOpenIdConfig	Grants permission to get the account details and OpenIdConfig attributes for your Amazon Chime account	Read			
GetAppInstanceRetentionSettings	Grants permission to get retention settings for an app instance	Read	app-instance*		
GetAppInstanceStreamingConfigurations	Grants permission to get the streaming configurations for an app instance	Read	app-instance*		
GetAttendee	Grants permission to get attendee details for a specified meeting ID and attendee ID	Read	meeting*		
GetBot	Grants permission to retrieve details for the specified bot	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCDRBucket	Grants permission to get details of a Call Detail Record S3 bucket associated with your Amazon Chime account	Read			s3:GetBucketAcl s3:GetBucketLocation s3:GetBucketLogging s3:GetBucketVersioning s3:GetBucketWebsite
GetChannelMembershipPreferences	Grants permission to get the preferences for a channel membership	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
GetChannelMessage	Grants permission to get the full details of a channel message	Read	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetChannelMessageStatus	Grants permission to get the status of a channel message	Read	app-instance-bot*		
			app-instance-user*		
			channel*		
GetDomain	Grants permission to get domain details for a domain associated with your Amazon Chime account	Read			
GetEventsConfiguration	Grants permission to retrieve details for an events configuration for a bot to receive outgoing events	Read			
GetGlobalSettings	Grants permission to get global settings related to Amazon Chime for the AWS account	Read			
GetMediaCapturePipeline	Grants permission to get an existing media capture pipeline	Read	media-pipeline*		
GetMediaInsightsPipelineConfiguration	Grants permission to get a media insights pipeline configuration	Read	media-insights-pipeline-configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMediaPipeline	Grants permission to get an existing media pipeline	Read	media-pipeline*		
GetMediaPipelineKinesisVideoStreamPool	Grants permission to get an existing media pipeline	Read	media-pipeline-kinesis-video-stream-pool*		
GetMeeting	Grants permission to get the meeting record for a specified meeting ID	Read	meeting*		
GetMeetingDetail	Grants permission to get attendee, connection, and other details for a meeting	Read			
GetMessagingSessionEndpoint	Grants permission to get the endpoint for the messaging session	Read			
GetMessagingStreamingConfigurations	Grants permission to get the data streaming configurations of an AppInstance	Read	app-instance*		
GetPhoneNumber	Grants permission to get details for the specified phone number	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPhoneNumberOrder	Grants permission to get details for the specified phone number order	Read			
GetPhoneNumberSettings	Grants permission to get phone number settings related to Amazon Chime for the AWS account	Read			
GetProxySession	Grants permission to get details of the specified proxy session for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetRetentionSettings	Grants permission to retrieve the retention settings for the specified Amazon Chime account	Read			
GetRoom	Grants permission to retrieve a room	Read			
GetSipMediaApplication	Grants permission to get details of Amazon Chime SIP media application under the administrator's AWS account	Read	sip-media-application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSipMediaApplicationAlexaSkillConfiguration	Grants permission to get Alexa Skill configuration settings for Amazon Chime SIP media application under the administrator's AWS account	Read	sip-media-application*		
GetSipMediaApplicationLoggingConfiguration	Grants permission to get logging configuration settings for Amazon Chime SIP media application under the administrator's AWS account	Read	sip-media-application*		
GetSipRule	Grants permission to get details of Amazon Chime SIP rule under the administrator's AWS account	Read			
GetSpeakerSearchTask	Grants permission to get a speaker search task on the specified Amazon Chime resource	Read	media-pipeline voice-connector		
GetTelephonyLimits	Grants permission to get telephony limits for the AWS account	Read			
GetUser	Grants permission to get details for the specified user ID	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserActivityReportData	Grants permission to get a summary of user activity on the user details page	Read			
GetUserByEmail	Grants permission to get user details for an Amazon Chime user based on the email address in an Amazon Chime Enterprise or Team account	Read			
GetUserSettings	Grants permission to get user settings related to the specified Amazon Chime user	Read			
GetVoiceConnector	Grants permission to get details for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceConnectorEmergencyCallingConfiguration	Grants permission to get details of the emergency calling configuration for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceConnectorExternalSystemsConfiguration	Grants permission to get the configuration of the external system that is connected with the specified Amazon Chime Voice Connector	Read	voice-connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVoiceConnectorGroup	Grants permission to get details for the specified Amazon Chime Voice Connector Group	Read			
GetVoiceConnectorLoggingConfiguration	Grants permission to get details of the logging configuration for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceConnectorOrigination	Grants permission to get details of the origination settings for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceConnectorProxy	Grants permission to get details of the proxy configuration for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceConnectorStreamingConfiguration	Grants permission to get details of the streaming configuration for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceConnectorTermination	Grants permission to get details of the termination settings for the specified Amazon Chime Voice Connector	Read	voice-connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVoiceConnectorTerminationHealth	Grants permission to get details of the termination health for the specified Amazon Chime Voice Connector	Read	voice-connector*		
GetVoiceProfile	Grants permission to get a voice profile	Read	voice-profile*		
GetVoiceProfileDomain	Grants permission to get a voice profile domain	Read	voice-profile-domain*		
GetVoiceToneAnalysisTask	Grants permission to get a voice tone analysis task on the specified Amazon Chime resource	Read	media-pipeline voice-connector		
InviteDelegate	Grants permission to send an invitation to accept a request for AWS account delegation for an Amazon Chime account	Write			
InviteUsers	Grants permission to invite as many as 50 users to the specified Amazon Chime account	Write			
InviteUsersFromProvider	Grants permission to invite users from a third party provider to your Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccountUsageReportData	Grants permission to list Amazon Chime account usage reporting data	List			
ListAccounts	Grants permission to list the Amazon Chime accounts under the administrator's AWS account	List			
ListApiKeys	Grants permission to list the SCIM access keys defined for your Amazon Chime account and Okta configuration	List			
ListAppInstanceAdmins	Grants permission to list administrators in the app instance	List	app-instance*		
			app-instance-bot*		
			app-instance-user*		
ListAppInstanceBots	Grants permission to list all AppInstanceBots created under a single app instance	List	app-instance-bot*		
ListAppInstanceUserEndpoints	Grants permission to list the endpoints registered for an app instance user	List	app-instance-user*		
ListAppInstanceUsers	Grants permission to list all AppInstanceUsers created under a single app instance	List	app-instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAppInstances	Grants permission to list all Amazon Chime app instances created under a single AWS account	List	app-instance*		
ListAttendeeTags	Grants permission to list the tags applied to an Amazon Chime SDK attendee resource	List	meeting*		
ListAttendees	Grants permission to list up to 100 attendees for a specified Amazon Chime SDK meeting	List	meeting*		
ListAvailableVoiceConnectorRegions	Grants permission to list the available AWS Regions in which you can create an Amazon Chime SDK Voice Connector	List			
ListBots	Grants permission to list the bots associated with the administrator's Amazon Chime Enterprise account	List			
ListCDRBucket	Grants permission to list Call Detail Record S3 buckets	List			s3:ListAllMyBuckets s3:ListBucket

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCallingRegions	Grants permission to list the calling regions available for the administrator's AWS account	List			
ListChannelBans	Grants permission to list all the users and bots banned from a particular channel	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelFlows	Grants permission to list all the Channel Flows created under a single Chime AppInstance	List	channel-flow*		
ListChannelMemberships	Grants permission to list all channel memberships in a channel	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannelMembershipsForAppInstanceUser	Grants permission to list all channels that a particular user or bot is a part of	List	app-instance-bot*		
			app-instance-user*		
ListChannelMessages	Grants permission to list all the messages in a channel	Read	app-instance-bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app-instance-user*		
			channel*		
ListChannelModerators	Grants permission to list all the moderators for a channel	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListChannels	Grants permission to list all the Channels created under a single Chime AppInstance	List	app-instance-bot*		
			app-instance-user*		
ListChannelsAssociatedWithChannelFlow	Grants permission to list all the Channels associated with a single Chime Channel Flow	List	channel-flow*		
ListChannelsModeratedByAppInstanceUser	Grants permission to list all channels moderated by a user or bot	List	app-instance-bot*		
			app-instance-user*		
ListDelegates	Grants permission to list account delegate information associated with your Amazon Chime account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDirectories	Grants permission to list active Active Directories hosted in the Directory Service of your AWS account	List			
ListDomains	Grants permission to list domains associated with your Amazon Chime account	List			
ListGroups	Grants permission to list Active Directory or Okta user groups associated with your Amazon Chime Enterprise account	List			
ListMediaCapturePipelines	Grants permission to list media capture pipelines	List			
ListMediaInsightsPipelineConfigurations	Grants permission to list all media insights pipeline configurations	List			
ListMediaPipelineKinesisVideoStreamPools	Grants permission to list media pipelines	List			
ListMediaPipelines	Grants permission to list media pipelines	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMeetingEvents	Grants permission to list all events that occurred for a specified meeting	List			
ListMeetingTags	Grants permission to list the tags applied to an Amazon Chime SDK meeting resource	List	meeting*		
ListMeetings	Grants permission to list up to 100 active Amazon Chime SDK meetings	List			
ListMeetingsReportData	Grants permission to list meetings ended during the specified date range	List			
ListPhoneNumberOrders	Grants permission to list the phone number orders under the administrator's AWS account	List			
ListPhoneNumbers	Grants permission to list the phone numbers under the administrator's AWS account	List			
ListProxySessions	Grants permission to list proxy sessions for the specified Amazon Chime Voice Connector	List	voice-connector*		
ListRoomMemberships	Grants permission to list all room members	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRooms	Grants permission to list rooms	List			
ListSipMediaApplications	Grants permission to list all Amazon Chime SIP media applications under the administrator's AWS account	List			
ListSipRules	Grants permission to list all Amazon Chime SIP rules under the administrator's AWS account	List	sip-media-application		
ListSubChannels	Grants permission to list all the SubChannels under a single Channel	List	app-instance-bot*		
			app-instance-user*		
			channel*		
ListSupportedPhoneNumberCountries	Grants permission to list the phone number countries supported by the AWS account	List			
ListTagsForResource	Grants permission to list the tags applied to an Amazon Chime resource	Read	app-instance		
			app-instance-bot		
			app-instance-user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			voice-profile-domain		
ListUsers	Grants permission to list the users that belong to the specified Amazon Chime account	List			
ListVoiceConnectorGroups	Grants permission to list the Amazon Chime Voice Connector Groups under the administrator's AWS account	List			
ListVoiceConnectorTerminationCredentials	Grants permission to list the SIP termination credentials for the specified Amazon Chime Voice Connector	List	voice-connector*		
ListVoiceConnectors	Grants permission to list the Amazon Chime Voice Connectors under the administrator's AWS account	List			
ListVoiceProfileDomains	Grants permission to list voice profile domains	List			
ListVoiceProfiles	Grants permission to list voice profiles	List	voice-profile-domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LogoutUser	Grants permission to log out the specified user from all of the devices they are currently logged into	Write			
PutAppInstanceRetentionSettings	Grants permission to enable data retention for the app instance	Write	app-instance*		
PutAppInstanceStreamingConfigurations	Grants permission to configure data streaming for the app instance	Write	app-instance*		
PutAppInstanceUserExpirationSettings	Grants permission to put expiration settings for an AppInstanceUser	Write	app-instance-user*		
PutChannelExpirationSettings	Grants permission to put expiration settings for a channel	Write	app-instance-user*		
			channel*		
PutChannelMembershipPreferences	Grants permission to put the preferences for a channel membership	Write	app-instance-bot*		
			app-instance-user*		
			channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEventsConfiguration	Grants permission to update details for an events configuration for a bot to receive outgoing events	Write			
PutMessagingStreamingConfigurations	Grants permission to put the data streaming configurations of an AppInstance	Write	app-instance*		
PutRetentionSettings	Grants permission to create or update retention settings for the specified Amazon Chime account	Write			
PutSipMediaApplicationAlexaSkillConfiguration	Grants permission to update Alexa Skill configuration settings for Amazon Chime SIP media application under the administrator's AWS account	Write	sip-media-application*		
PutSipMediaApplicationLoggingConfiguration	Grants permission to update logging configuration settings for Amazon Chime SIP media application under the administrator's AWS account	Write	sip-media-application*		
PutVoiceConnectorEmergencyCallingConfiguration	Grants permission to add emergency calling configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutVoiceConnectorExternalSystemsConfiguration	Grants permission to update the configuration of the external system that is connected with the specified Amazon Chime Voice Connector	Write	voice-connector*		
PutVoiceConnectorLoggingConfiguration	Grants permission to add logging configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:GetLogDelivery logs:ListLogDeliveries

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutVoiceConnectorOrigination	Grants permission to update the origination settings for the specified Amazon Chime Voice Connector	Write	voice-connector*		
PutVoiceConnectorProxy	Grants permission to add proxy configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		
PutVoiceConnectorStreamingConfiguration	Grants permission to add streaming configuration for the specified Amazon Chime Voice Connector	Write	voice-connector*		chime:GetMediaInsightsPipelineConfiguration
			media-insights-pipeline-configuration		
PutVoiceConnectorTermination	Grants permission to update the termination settings for the specified Amazon Chime Voice Connector	Write	voice-connector*		
PutVoiceConnectorTerminationCredentials	Grants permission to add SIP termination credentials for the specified Amazon Chime Voice Connector	Write	voice-connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RedactChannelMessage	Grants permission to redact message content	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
RedactConversationMessage	Grants permission to redact the specified Chime conversation Message	Write			
RedactRoomMessage	Grants permission to redacts the specified Chime room Message	Write			
RegenerateSecurityToken	Grants permission to regenerate the security token for the specified bot	Write			
RegisterAppInstanceUserEndpoint	Grants permission to register an endpoint for an app instance user	Write	app-instance-user*		mobiletargeting:GetApp
RenameAccount	Grants permission to modify the account name for your Amazon Chime Enterprise or Team account	Write			
RenewDelegate	Grants permission to renew the delegation request associated with an Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetAccountResource	Grants permission to reset the account resource in your Amazon Chime account	Write			
ResetPersonalPIN	Grants permission to reset the personal meeting PIN for the specified user on an Amazon Chime account	Write			
RestorePhoneNumber	Grants permission to restore the specified phone number from the deltion queue back to the phone number inventory	Write			
RetrieveDataExports	Grants permission to download the file containing links to all user attachments returned as part of the "Request attachments" action	Read			
SearchAvailablePhoneNumbers	Grants permission to search phone numbers that can be ordered from the carrier	Read			
SearchChannels	Grants permission to search channels that an AppInstanceUser belongs to, or search channels across the AppInstance for an AppInstaceAdmin	List	app-instance-bot* app-instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendChannelMessage	Grants permission to send a message to a particular channel that the member is a part of	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
StartDataExport	Grants permission to submit the "Request attachments" request	Write			
StartMeetingTranscription	Grants permission to start transcription for a meeting	Write			
StartSpeakerSearchTask	Grants permission to start a speaker search task on the specified Amazon Chime resource	Write	media-pipeline		
			voice-connector		
StartVoiceToneAnalysisTask	Grants permission to start a voice tone analysis task on the specified Amazon Chime resource	Write	media-pipeline		
			voice-connector		
StopMeetingTranscription	Grants permission to stop transcription for a meeting	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopSpeakerSearchTask	Grants permission to stop a speaker search task on the specified Amazon Chime resource	Write	media-pipeline		
			voice-connector		
StopVoiceToneAnalysisTask	Grants permission to stop a voice tone analysis task on the specified Amazon Chime resource	Write	media-pipeline		
			voice-connector		
SubmitSupportRequest	Grants permission to submit a customer service support request	Write			
SuspendUsers	Grants permission to suspend users from an Amazon Chime Enterprise account	Write			
TagAttendee	Grants permission to apply the specified tags to the specified Amazon Chime SDK attendee	Tagging	meeting*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagMeeting	Grants permission to apply the specified tags to the specified Amazon Chime SDK meeting	Tagging	meeting*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Grants permission to apply the specified tags to the specified resource (tag-based access controls are only supported on *-chime.<region>.amazonaws.com endpoints)	Tagging	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		
			sip-media-application		
			voice-connector		
			voice-profile-domain		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnauthorizeDirectory	Grants permission to unauthorize an Active Directory from your Amazon Chime Enterprise account	Write			
UntagAttendee	Grants permission to untag the specified tags from the specified Amazon Chime SDK attendee	Tagging	meeting*		
UntagMeeting	Grants permission to untag the specified tags from the specified Amazon Chime SDK meeting	Tagging	meeting*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag the specified tags from the specified resource (tag-based access controls are only supported on *-chime.<region>.amazonaws.com endpoints)	Tagging	app-instance		
			app-instance-bot		
			app-instance-user		
			channel		
			channel-flow		
			media-insights-pipeline-configuration		
			media-pipeline		
			media-pipeline-kinesis-video-stream-pool		
			meeting		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			sip-media-application		
			voice-connector		
			voice-profile-domain		
				aws:TagKeys	
UpdateAccount	Grants permission to update account details for the specified Amazon Chime account	Write			
UpdateAccountOpenIdConfig	Grants permission to update the OpenIdConfig attributes for your Amazon Chime account	Write			
UpdateAccountResource	Grants permission to update the account resource in your Amazon Chime account	Write			
UpdateAccountSettings	Grants permission to update the settings for the specified Amazon Chime account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAppInstance	Grants permission to update AppInstance metadata	Write	app-instance*		
UpdateAppInstanceBot	Grants permission to update the details for an AppInstanceBot	Write	app-instance-bot*		
UpdateAppInstanceUser	Grants permission to update the details for an AppInstanceUser	Write	app-instance-user*		
UpdateAppInstanceUserEndpoint	Grants permission to update an endpoint registered for an app instance user	Write	app-instance-user*		
UpdateAttendeeCapabilities	Grants permission to the capabilties that you want to update	Write	meeting*		
UpdateBot	Grants permission to update the status of the specified bot	Write			
UpdateCDRSettings	Grants permission to update your Call Detail Record S3 bucket	Write			s3:CreateBucket s3:DeleteBucket s3:ListAllMyBuckets
UpdateChannel	Grants permission to update a channel's attributes	Write	app-instance-bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app-instance-user*		
			channel*		
UpdateChannelFlow	Grants permission to update a channel flow	Write	channel-flow*		
UpdateChannelMessage	Grants permission to update the content of a message	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateChannelReadMarker	Grants permission to set the timestamp to the point when a user last read messages in a channel	Write	app-instance-bot*		
			app-instance-user*		
			channel*		
UpdateGlobalSettings	Grants permission to update the global settings related to Amazon Chime for the AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMediaInsightsPipelineConfiguration	Grants permission to update the status of a media insights pipeline configuration	Write	media-insights-pipeline-configuration*		chime:ListVoiceConnectors iam:PassRole kinesis:DescribeStream s3:ListBucket
UpdateMediaInsightsPipelineStatus	Grants permission to update the status of a media insights pipeline	Write	media-pipeline*		
UpdateMediaPipelineKinesisVideoStreamPool	Grants permission to update kinesis video stream pool	Write	media-pipeline-kinesis-video-stream-pool*		
UpdatePhoneNumber	Grants permission to update phone number details for the specified phone number	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePhoneNumberSettings	Grants permission to update phone number settings related to Amazon Chime for the AWS account	Write			
UpdateProxySession	Grants permission to update a proxy session for the specified Amazon Chime Voice Connector	Write	voice-connector*		
UpdateRoom	Grants permission to update a room	Write			
UpdateRoomMembership	Grants permission to update room membership role	Write			
UpdateSipMediaApplication	Grants permission to update properties of Amazon Chime SIP media application under the administrator's AWS account	Write	sip-media-application*		
UpdateSipMediaApplicationCall	Grants permission to update an Amazon Chime SIP media application call under the administrator's AWS account	Write	sip-media-application*		
UpdateSipRule	Grants permission to update properties of Amazon Chime SIP rule under the administrator's AWS account	Write	sip-media-application		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSupportedLicenses	Grants permission to update the supported license tiers available for users in your Amazon Chime account	Write			
UpdateUser	Grants permission to update user details for a specified user ID	Write			
UpdateUserLicenses	Grants permission to update the licenses for your Amazon Chime users	Write			
UpdateUserSettings	Grants permission to update user settings related to the specified Amazon Chime user	Write			
UpdateVoiceConnector	Grants permission to update Amazon Chime Voice Connector details for the specified Amazon Chime Voice Connector	Write	voice-connector*		
UpdateVoiceConnectorGroup	Grants permission to update Amazon Chime Voice Connector Group details for the specified Amazon Chime Voice Connector Group	Write	voice-connector		
UpdateVoiceProfile	Grants permission to update a voice profile	Write	voice-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVoiceProfileDomain	Grants permission to update a voice profile domain	Write	voice-profile-domain*		
ValidateAccountResource	Grants permission to validate the account resource in your Amazon Chime account	Read			
ValidateE911Address	Grants permission to validate an address to be used for 911 calls made with Amazon Chime Voice Connectors	Read			

Resource types defined by Amazon Chime

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
meeting	`arn:${Partition}:chime:${Region}:${AccountId}:meeting/${MeetingId}`	aws:ResourceTag/${TagKey}
app-instance	`arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
app-instance-user	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/user/${AppInstanceUserId}	aws:ResourceTag/${TagKey}
app-instance-bot	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/bot/${AppInstanceBotId}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel/${ChannelId}	aws:ResourceTag/${TagKey}
channel-flow	arn:${Partition}:chime:${Region}:${AccountId}:app-instance/${AppInstanceId}/channel-flow/${ChannelFlowId}	aws:ResourceTag/${TagKey}
media-pipeline	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline/${MediaPipelineId}	aws:ResourceTag/${TagKey}
media-insights-pipeline-configuration	arn:${Partition}:chime:${Region}:${AccountId}:media-insights-pipeline-configuration/${ConfigurationName}	aws:ResourceTag/${TagKey}
media-pipeline-kinesis-video-stream-pool	arn:${Partition}:chime:${Region}:${AccountId}:media-pipeline-kinesis-video-stream-pool/${PoolName}	aws:ResourceTag/${TagKey}
voice-profile-domain	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile-domain/${VoiceProfileDomainId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
voice-profile	arn:${Partition}:chime:${Region}:${AccountId}:voice-profile/${VoiceProfileId}	
voice-connector	arn:${Partition}:chime:${Region}:${AccountId}:vc/${VoiceConnectorId}	aws:ResourceTag/${TagKey}
sip-media-application	arn:${Partition}:chime:${Region}:${AccountId}:sma/${SipMediaApplicationId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Chime

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

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

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

Actions, resources, and condition keys for AWS Clean Rooms

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

References:

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

Topics

Actions defined by AWS Clean Rooms

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

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

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

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetCollaborationAnalysisTemplate	Grants permission to view details of analysisTemplates associated to the collaboration	Read	analysistemplate*		cleanrooms:GetCollaborationAnalysisTemplate
			collaboration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetSchema	Grants permission to view details for schemas	Read	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
BatchGetSchemaAnalysisRule	Grants permission to view analysis rules associated with schemas	Read	collaboration*		cleanrooms:GetSchema
			configuredtableassociation		
			idmappingtable		
CreateAnalysisTemplate	Grants permission to create a new analysis template	Write	analysistemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollaboration	Grants permission to create a new collaboration, a shared data collaboration environment	Write	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCollaborationChangeRequest	Grants permission to create a change request in a collaboration	Write	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfiguredAudienceModelAssociation	Grants permission to link a Cleanrooms ML configured audience model with a collaboration by creating a new association	Write	configuredaudiencemodelassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	cleanrooms-ml:GetConfiguredAudienceModel cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfiguredTable	Grants permission to create a new configured table	Write	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	athena:GetTableMetadata glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions glue:GetSchemaVersion glue:GetTable glue:GetTables
CreateConfiguredTableAnalysisRule	Grants permission to create a analysis rule for a configured table	Write	configuredtable*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfiguredTableAssociation	Grants permission to link a configured table with a collaboration by creating a new association	Write	configuredtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole
			configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateConfiguredTableAssociationAnalysisRule	Grants permission to create an analysis rule for a configured table association	Write	configuredtableassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIdMappingTable	Grants permission to link an id mapping workflow with a collaboration by creating a new id mapping table	Write	idmappingtable*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdMappingWorkflow
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIdNamespaceAssociation	Grants permission to link an AWS Entity Resolution Id Namespace with a collaboration by creating a new association	Write	idnamespaceassociation*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	entityresolution:AddPolicyStatement entityresolution:GetIdNamespace
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMembership	Grants permission to join collaborations by creating a membership	Write	collaboration*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
			membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePrivacyBudgetTemplate	Grants permission to create a new privacy budget template	Write	membership*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
			privacybudgettemplate*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteAnalysisTemplate	Grants permission to delete an existing analysis template	Write	analysistemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCollaboration	Grants permission to delete an existing collaboration	Write	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfiguredAudienceModelAssociation	Grants permission to delete an existing configured audience model association	Write	configuredaudiencemodelassociation*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteConfiguredTable	Grants permission to delete a configured table	Write	configuredtable*		
DeleteConfiguredTableAnalysisRule	Grants permission to delete an existing analysis rule	Write	configuredtable*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfiguredTableAssociation	Grants permission to remove a configured table association from a collaboration	Write	configuredtableassociation*		
DeleteConfiguredTableAssociationAnalysisRule	Grants permission to delete an existing configured table association analysis rule	Write	configuredtableassociation*		
DeleteIdMappingTable	Grants permission to remove an id mapping table from a collaboration	Write	idmappingtable*		entityresolution:DeletePolicyStatement
			membership*		
DeleteIdNamespaceAssociation	Grants permission to remove an Id Namespace Association from a collaboration	Write	idnamespaceassociation*		entityresolution:DeletePolicyStatement
			membership*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMember	Grants permission to delete members from a collaboration	Write	collaboration*		cleanrooms-ml:DeleteConfiguredAudienceModelPolicy cleanrooms-ml:GetConfiguredAudienceModelPolicy cleanrooms-ml:PutConfiguredAudienceModelPolicy
DeleteMembership	Grants permission to leave collaborations by deleting a membership	Write	membership*		
DeletePrivacyBudgetTemplate	Grants permission to delete an existing privacy budget template	Write	privacybudgettemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAnalysisTemplate	Grants permission to view details for an analysis template	Read	analysistemplate*		
GetCollaboration	Grants permission to view details for a collaboration	Read	collaboration*		
GetCollaborationAnalysisTemplate	Grants permission to view details for an analysis template within a collaboration	Read	analysistemplate*		
			collaboration*		
GetCollaborationChangeRequest	Grants permission to get a change request in a collaboration	Read	collaboration*		
GetCollaborationConfiguredAudienceModelAssociation	Grants permission to view details for a configured audience model association within a collaboration	Read	collaboration*		
			configuredaudiencemodelassociation*		
GetCollaborationIdNamespaceAssociation	Grants permission to get id namespace association within a collaboration	Read	collaboration*		
			idnamespaceassociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCollaborationPrivacyBudgetTemplate	Grants permission to view details for a privacy budget template within a collaboration	Read	collaboration*		
			privacybudgettemplate*		
GetConfiguredAudienceModelAssociation	Grants permission to view details for a configured audience model association	Read	configuredaudiencemodelassociation*		
GetConfiguredTable	Grants permission to view details for a configured table	Read	configuredtable*		
GetConfiguredTableAnalysisRule	Grants permission to view analysis rules for a configured table	Read	configuredtable*		
GetConfiguredTableAssociation	Grants permission to view details for a configured table association	Read	configuredtableassociation*		
GetConfiguredTableAssociationAnalysisRule	Grants permission to view analysis rules for a configured table association	Read	configuredtableassociation*		
GetIdMappingTable	Grants permission to view details of an id mapping table	Read	idmappingtable*		
			membership*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdNamespaceAssociation	Grants permission to view details of an id namespace association	Read	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		
GetMembership	Grants permission to view details about a membership	Read	membership*		
GetPrivacyBudgetTemplate	Grants permission to view details for a privacy budget template	Read	privacybudgettemplate*		
GetProtectedJob	Grants permission to view a protected job	Read	membership*		
GetProtectedQuery	Grants permission to view a protected query	Read	membership*		
GetSchema	Grants permission to view details for a schema	Read	collaboration*		
			configuredtableassociation*		
GetSchemaAnalysisRule	Grants permission to view analysis rules associated with a schema	Read	collaboration*		cleanrooms:GetSchema

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configuredtableassociation*		
ListAnalysisTemplates	Grants permission to list available analysis templates	List	analysistemplate*		
			membership*		
ListCollaborationAnalysisTemplates	Grants permission to list available analysis templates within a collaboration	List	collaboration*		
ListCollaborationChangeRequests	Grants permission to list change requests in a collaboration	List	collaboration*		
ListCollaborationConfiguredAudienceModelAssociations	Grants permission to list available configured audience model association within a collaboration	List	collaboration*		
ListCollaborationIdNamespaceAssociations	Grants permission to list id namespace within a collaboration	List	collaboration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCollaborationPrivacyBudgetTemplates	Grants permission to list available privacy budget templates within a collaboration	List	collaboration*		
ListCollaborationPrivacyBudgets	Grants permission to list privacy budgets within a collaboration	List	collaboration*		
ListCollaborations	Grants permission to list available collaborations	List			
ListConfiguredAudienceModelAssociations	Grants permission to list available configured audience model associations for a membership	List	configuredaudiencemodelassociation*		
			membership*		
ListConfiguredTableAssociations	Grants permission to list available configured table associations for a membership	List	configuredtableassociation*		
			membership*		
ListConfiguredTables	Grants permission to list available configured tables	List			
ListIdMappingTables	Grants permission to list available id mapping tables for a membership	List	idmappingtable*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			membership*		
ListIdNamespaceAssociations	Grants permission to list entity resolution data associations for a membership	List	idnamespaceassociation*		
			membership*		
ListMembers	Grants permission to list the members of a collaboration	List	collaboration*		
ListMemberships	Grants permission to list available memberships	List			
ListPrivacyBudgetTemplates	Grants permission to list available privacy budget templates	List	membership*		
			privacybudgettemplate*		
ListPrivacyBudgets	Grants permission to list available privacy budgets	List	membership*		
ListProtectedJobs	Grants permission to list protected jobs	List	membership*		
ListProtectedQueries	Grants permission to list protected queries	List	membership*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSchemas	Grants permission to view available schemas for a collaboration	List	collaboration*		
ListTagsForResource	Grants permission to list tags for a resource	List	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			membership		
			privacybudgettemplate		
PassCollaboration [permission only]	Grants permission to access a collaboration in the context of Clean Rooms ML custom models	Read	collaboration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PassMembership [permission only]	Grants permission to access a membership in the context of Clean Rooms ML custom models	Read	membership*		
PopulateIdMappingTable	Grants permission to start an Id Mapping Job in AWS Entity Resolution to generate id mapping results in cleanrooms collaboration.	Write	idmappingtable*		entityresolution:GetIdMappingWorkflow
			membership*		
PreviewPrivacyImpact	Grants permission to preview privacy budget template settings	Read	membership*		
StartProtectedJob	Grants permission to start protected jobs	Write	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema
			analysistemplate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configuredtableassociation		
StartProtectedQuery	Grants permission to start protected queries	Write	membership*		cleanrooms:GetCollaborationAnalysisTemplate cleanrooms:GetSchema s3:GetBucketLocation s3:ListBucket s3:PutObject
			analysistemplate		
			configuredtableassociation		
			idmappingtable		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		
			membership		
			privacybudgettemplate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	analysistemplate		
			collaboration		
			configuredaudiencemodelassociation		
			configuredtable		
			configuredtableassociation		
			idmappingtable		
			idnamespaceassociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			membership		
			privacybudgettemplate		
				aws:TagKeys	
UpdateAnalysisTemplate	Grants permission to update details of the analysis template	Write	analysistemplate*		
UpdateCollaboration	Grants permission to update details of the collaboration	Write	collaboration*		
UpdateCollaborationChangeRequest	Grants permission to update a change request in a collaboration	Write	collaboration*		
UpdateConfiguredAudienceModelAssociation	Grants permission to update a configured audience model association	Write	configuredaudiencemodelassociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConfiguredTable	Grants permission to update an existing configured table	Write	configuredtable*		athena:GetTableMetadata cleanrooms:UpdateConfiguredTableAllowedColumns cleanrooms:UpdateConfiguredTableReference glue:BatchGetPartition glue:GetDatabase glue:GetDatabases glue:GetPartition glue:GetPartitions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					glue:GetSchemaVersion glue:GetTable glue:GetTables
UpdateConfiguredTableAllowedColumns [permission only]	Grants permission to update the allowed columns of an existing configured table	Write	configuredtable*		
UpdateConfiguredTableAnalysisRule	Grants permission to update analysis rules for a configured table	Write	configuredtable*		
UpdateConfiguredTableAssociation	Grants permission to update a configured table association	Write	configuredtableassociation*		iam:PassRole
UpdateConfiguredTableAssociationAnalysisRule	Grants permission to update analysis rules for a configured table association	Write	configuredtableassociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConfiguredTableReference [permission only]	Grants permission to update the table reference of an existing configured table	Write	configuredtable*		
UpdateIdMappingTable	Grants permission to update an id mapping table	Write	idmappingtable*		
			membership*		
UpdateIdNamespaceAssociation	Grants permission to update a entity resolution input association	Write	idnamespaceassociation*		entityresolution:GetIdNamespace
			membership*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMembership	Grants permission to update details of a membership	Write	membership*		iam:PassRole logs:CreateLogDelivery logs:CreateLogGroup logs:DeleteLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					logs:PutResourcePolicy logs:UpdateLogDelivery s3:GetBucketLocation
UpdatePrivacyBudgetTemplate	Grants permission to update details of the privacy budget template	Write	privacybudgettemplate*		
UpdateProtectedJob	Grants permission to update protected jobs	Write	membership*		
UpdateProtectedQuery	Grants permission to update protected queries	Write	membership*		

Resource types defined by AWS Clean Rooms

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
analysistemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/analysistemplate/${AnalysisTemplateId}	aws:ResourceTag/${TagKey}
collaboration	arn:${Partition}:cleanrooms:${Region}:${Account}:collaboration/${CollaborationId}	aws:ResourceTag/${TagKey}
configuredaudiencemodelassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredaudiencemodelassociation/${ConfiguredAudienceModelAssociationId}	aws:ResourceTag/${TagKey}
configuredtable	arn:${Partition}:cleanrooms:${Region}:${Account}:configuredtable/${ConfiguredTableId}	aws:ResourceTag/${TagKey}
configuredtableassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/configuredtableassociation/${ConfiguredTableAssociationId}	aws:ResourceTag/${TagKey}
idmappingtable	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idmappingtable/${IdMappingTableId}	aws:ResourceTag/${TagKey}
idnamespaceassociation	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/idnamespaceassociation/${IdNamespaceAssociationId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
membership	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}	aws:ResourceTag/${TagKey}
privacybudgettemplate	arn:${Partition}:cleanrooms:${Region}:${Account}:membership/${MembershipId}/privacybudgettemplate/${PrivacyBudgetTemplateId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Clean Rooms

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

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

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Clean Rooms ML

AWS Clean Rooms ML (service prefix: `cleanrooms-ml`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Clean Rooms ML

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTrainedModel	Grants permission to cancel a trained model	Write	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTrainedModelInferenceJob	Grants permission to cancel a trained model inference job	Write	TrainedModelInferenceJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAudienceModel	Grants permission to create an audience model	Write	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredAudienceModel	Grants permission to create a configured audience model	Write	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfiguredModelAlgorithm	Grants permission to create a configured model algorithm	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguredModelAlgorithmAssociation	Grants permission to create a configured model algorithm association	Write	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMLInputChannel	Grants permission to create an ML input channel	Write	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrainedModel	Grants permission to create a trained model	Write	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingDataset	Grants permission to create a training dataset, or seed audience. In Clean Rooms ML, the TrainingDataset is metadata that points to a Glue table, which is read only during AudienceModel creation	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAudienceGenerationJob	Grants permission to delete the specified audience generation job, and removes all data associated with the job	Write	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAudienceModel	Grants permission to delete the specified audience generation job, and removes all data associated with the job	Write	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModel	Grants permission to delete the specified configured audience model	Write	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredAudienceModelPolicy	Grants permission to delete the specified configured audience model policy	Write	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfiguredModelAlgorithm	Grants permission to delete a configured model algorithm	Write	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfiguredModelAlgorithmAssociation	Grants permission to delete a configured model algorithm association	Write	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMLConfiguration	Grants permission to delete an ML configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMLInputChannelData	Grants permission to delete all data associated with the ML input channel	Write	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainedModelOutput	Grants permission to delete all output associated with the trained model	Write	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTrainingDataset	Grants permission to delete a training dataset	Write	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAudienceGenerationJob	Grants permission to return information about an audience generation job	Read	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAudienceModel	Grants permission to return information about an audience model	Read	audiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCollaborationConfiguredModelAlgorithmAssociation	Grants permission to return information about a configured model algorithm association created by any member in the collaboration	Read	ConfiguredModelAlgorithmAssociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetCollaborationMLInputChannel	Grants permission to return information about an ML input channel created by any member in the collaboration	Read	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetCollaborationTrainedModel	Grants permission to return information about a trained model created by any member in the collaboration	Read	TrainedModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
GetConfiguredAudienceModel	Grants permission to return information about a configured audience model	Read	configuredaudiencemodel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredAudienceModelPolicy	Grants permission to return information about a configured audience model policy	Read	configuredaudiencemodel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithm	Grants permission to return information about a configured model algorithm	Read	ConfiguredModelAlgorithm*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetConfiguredModelAlgorithmAssociation	Grants permission to return information about a configured model algorithm association	Read	ConfiguredModelAlgorithmAssociation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMLConfiguration	Grants permission to return information about an ML configuration	Read		aws:RequestTag/${TagKey} aws:TagKeys	
GetMLInputChannel	Grants permission to return information about an ML input channel	Read	MLInputChannel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModel	Grants permission to return information about a trained model	Read	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainedModelInferenceJob	Grants permission to return information about a trained model inference job	Read	TrainedModelInferenceJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
GetTrainingDataset	Grants permission to return information about a training dataset	Read	trainingdataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceExportJobs	Grants permission to return a list of the audience export jobs	List	audiencegeneration job		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceGenerationJobs	Grants permission to return a list of audience generation jobs	List	configuredaudiencemodel		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ListAudienceModels	Grants permission to return a list of audience models	List			
ListCollaborationConfiguredModelAlgorithmAssociations	Grants permission to return a list of configured model algorithms created by any member in the collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCollaborationMLInputChannels	Grants permission to return a list of ML input channels created by any member in the collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModelExportJobs	Grants permission to return a list of trained model export jobs started by any member in the collaboration	List	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCollaborationTrainedModelInferenceJobs	Grants permission to return a list of trained model inference jobs started by any member in the collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListCollaborationTrainedModels	Grants permission to return a list of trained models created by any member in the collaboration	List		aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
ListConfiguredAudienceModels	Grants permission to return a list of configured audience models	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfiguredModelAlgorithmAssociations	Grants permission to return a list of configured model algorithm associations	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListConfiguredModelAlgorithms	Grants permission to return a list of configured model algorithms	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListMLInputChannels	Grants permission to return a list of ML input channels	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTagsForResource	Grants permission to return a list of tags for a provided resource	List	audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
ListTrainedModelInferenceJobs	Grants permission to return a list of trained model inference jobs	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModelVersions	Grants permission to return a list of trained model versions	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListTrainedModels	Grants permission to return a list of trained models	List		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrainingDatasets	Grants permission to return a list of training datasets	List			
PutConfiguredAudienceModelPolicy	Grants permission to create or update the resource policy for a configured audience model	Permissions management	configuredaudiencemodel*		
PutMLConfiguration	Grants permission to put an ML configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceExportJob	Grants permission to export an audience of a specified size after you have generated an audience	Write	audiencegenerationjob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAudienceGenerationJob	Grants permission to start the audience generation job	Write	configuredaudiencemodel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys cleanrooms-ml:CollaborationId	
StartTrainedModelExportJob	Grants permission to start a trained model export job	Write	TrainedModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartTrainedModelInferenceJob	Grants permission to start a trained model inference job	Write	ConfiguredModelAlgorithmAssociation*		
			MLInputChannel*		
			TrainedModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to tag a specific resource	Tagging	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UnTagResource	Grants permission to untag a specific resource	Tagging	ConfiguredModelAlgorithm		
			ConfiguredModelAlgorithmAssociation		
			MLInputChannel		
			TrainedModel		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			TrainedModelInferenceJob		
			audiencegenerationjob		
			audiencemodel		
			configuredaudiencemodel		
			trainingdataset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConfiguredAudienceModel	Grants permission to update a configured audience model.	Write	configuredaudiencemodel*		
			audiencemodel		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	

Resource types defined by AWS Clean Rooms ML

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
trainingdataset	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:training-dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
audiencemodel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-model/${ResourceId}`	aws:ResourceTag/${TagKey}
configuredaudiencemodel	`arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-audience-model/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
audiencegenerationjob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:audience-generation-job/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithm	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:configured-model-algorithm/${ResourceId}	aws:ResourceTag/${TagKey}
ConfiguredModelAlgorithmAssociation	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/configured-model-algorithm-association/${ResourceId}	aws:ResourceTag/${TagKey}
MLInputChannel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/ml-input-channel/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModel	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model/${ResourceId}	aws:ResourceTag/${TagKey}
TrainedModelInferenceJob	arn:${Partition}:cleanrooms-ml:${Region}:${Account}:membership/${MembershipId}/trained-model-inference-job/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Clean Rooms ML

AWS Clean Rooms ML defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
cleanrooms-ml:CollaborationId	Filters access by Clean rooms collaboration id	String

Actions, resources, and condition keys for AWS Cloud Control API

AWS Cloud Control API (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 AWS Cloud Control API
- Resource types defined by AWS Cloud Control API
- Condition keys for AWS Cloud Control API

Actions defined by AWS Cloud Control API

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelResourceRequest	Grants permission to cancel resource requests in your account	Write			
CreateResource	Grants permission to create resources in your account	Write			
DeleteResource	Grants permission to delete resources in your account	Write			
GetResource	Grants permission to get resources in your account	Read			
GetResourceRequestStatus	Grants permission to get resource requests in your account	Read			
ListResourceRequests	Grants permission to list resource requests in your account	Read			
ListResources	Grants permission to list resources in your account	Read			
UpdateResource	Grants permission to update resources in your account	Write			

Resource types defined by AWS Cloud Control API

AWS Cloud Control API does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Cloud Control API, specify `"Resource": "*"` in your policy.

Condition keys for AWS Cloud Control API

Cloud Control API has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Cloud Directory

Amazon Cloud Directory (service prefix: `clouddirectory`) 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 Cloud Directory
- Resource types defined by Amazon Cloud Directory
- Condition keys for Amazon Cloud Directory

Actions defined by Amazon Cloud Directory

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddFacetToObject	Grants permission to add a new Facet to an object	Write	directory*		
ApplySchema	Grants permission to copy input published schema into Directory with same name and version as that of published schema	Write	directory* publishedSchema*		
AttachObject	Grants permission to attach an existing object to another existing object	Write	directory*		
AttachPolicy	Grants permission to attach a policy object to any other object	Write	directory*		
AttachToIndex	Grants permission to attach the specified object to the specified index	Write	directory*		
AttachTypedLink	Grants permission to attach a typed link b/w a source & target object reference	Write	directory*		
BatchRead	Grants permission to perform all the read operations in a batch. Each individual operation inside BatchRead needs to be granted permissions explicitly	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchWrite	Grants permission to perform all the write operations in a batch. Each individual operation inside BatchWrite needs to be granted permissions explicitly	Write	directory*		
CreateDirectory	Grants permission to create a Directory by copying the published schema into the directory	Write	publishedSchema*		
CreateFacet	Grants permission to create a new Facet in a schema	Write	appliedSchema*		
			developmentSchema*		
CreateIndex	Grants permission to create an index object	Write	directory*		
CreateObject	Grants permission to create an object in a Directory	Write	directory*		
CreateSchema	Grants permission to create a new schema in a development state	Write			
CreateTypedLinkFacet	Grants permission to create a new Typed Link facet in a schema	Write	appliedSchema*		
			developmentSchema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDirectory	Grants permission to delete a directory. Only disabled directories can be deleted	Write	directory*		
DeleteFacet	Grants permission to delete a given Facet. All attributes and Rules associated with the facet will be deleted	Write	developmentSchema*		
DeleteObject	Grants permission to delete an object and its associated attributes	Write	directory*		
DeleteSchema	Grants permission to delete a given schema	Write	developmentSchema*		
			publishedSchema*		
DeleteTypedLinkFacet	Grants permission to delete a given TypedLink Facet. All attributes and Rules associated with the facet will be deleted	Write	developmentSchema*		
DetachFromIndex	Grants permission to detach the specified object from the specified index	Write	directory*		
DetachObject	Grants permission to detach a given object from the parent object	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachPolicy	Grants permission to detach a policy from an object	Write	directory*		
DetachTypedLink	Grants permission to detach a given typed link b/w given source and target object reference	Write	directory*		
DisableDirectory	Grants permission to disable the specified directory	Write	directory*		
EnableDirectory	Grants permission to enable the specified directory	Write	directory*		
GetAppliedSchemaVersion	Grants permission to return current applied schema version ARN, including the minor version in use	Read	appliedSchema*		
GetDirectory	Grants permission to retrieve metadata about a directory	Read	directory*		
GetFacet	Grants permission to get details of the Facet, such as Facet Name, Attributes, Rules, or ObjectType	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetLinkAttributes	Grants permission to retrieve attributes that are associated with a typed link	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectAttributes	Grants permission to retrieve attributes within a facet that are associated with an object	Read	directory*		
GetObjectInformation	Grants permission to retrieve metadata about an object	Read	directory*		
GetSchemaAsJson	Grants permission to retrieve a JSON representation of the schema	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
GetTypedLinkFacetInformation	Grants permission to return identity attributes order information associated with a given typed link facet	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListAppliedSchemaArns	Grants permission to list schemas applied to a directory	List	directory*		
ListAttachedIndices	Grants permission to list indices attached to an object	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDevelopmentSchemaArns	Grants permission to retrieve the ARNs of schemas in the development state	List			
ListDirectories	Grants permission to list directories created within an account	List			
ListFacetAttributes	Grants permission to retrieve attributes attached to the facet	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListFacetNames	Grants permission to retrieve the names of facets that exist in a schema	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListIncomingTypedLinks	Grants permission to return a paginated list of all incoming TypedLinks for a given object	Read	directory*		
ListIndex	Grants permission to list objects attached to the specified index	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListManagedSchemaArns	Grants permission to list the major version families of each managed schema. If a major version ARN is provided as SchemaArn, the minor version revisions in that family are listed instead	List			
ListObjectAttributes	Grants permission to list all attributes associated with an object	Read	directory*		
ListObjectChildren	Grants permission to return a paginated list of child objects associated with a given object	Read	directory*		
ListObjectParentPaths	Grants permission to retrieve all available parent paths for any object type such as node, leaf node, policy node, and index node objects	Read	directory*		
ListObjectParents	Grants permission to list parent objects associated with a given object in pagination fashion	Read	directory*		
ListObjectPolicies	Grants permission to return policies attached to an object in pagination fashion	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOutgoingTypedLinks	Grants permission to return a paginated list of all outgoing TypedLinks for a given object	Read	directory*		
ListPolicyAttachments	Grants permission to return all of the ObjectIdentifiers to which a given policy is attached	Read	directory*		
ListPublishedSchemaArns	Grants permission to retrieve published schema ARNs	List			
ListTagsForResource	Grants permission to return tags for a resource	Read	directory*		
ListTypedLinkFacetAttributes	Grants permission to return a paginated list of attributes associated with typed link facet	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		
ListTypedLinkFacetNames	Grants permission to return a paginated list of typed link facet names that exist in a schema	Read	appliedSchema*		
			developmentSchema*		
			publishedSchema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LookupPolicy	Grants permission to list all policies from the root of the Directory to the object specified	Read	directory*		
PublishSchema	Grants permission to publish a development schema with a version	Write	developmentSchema*		
PutSchemaFromJson	Grants permission to update a schema using JSON upload. Only available for development schemas	Write			
RemoveFacetFromObject	Grants permission to remove the specified facet from the specified object	Write	directory*		
TagResource	Grants permission to add tags to a resource	Tagging	directory*		
UntagResource	Grants permission to remove tags from a resource	Tagging	directory*		
UpdateFacet	Grants permission to add/update/delete existing Attributes, Rules, or ObjectType of a Facet	Write	appliedSchema*		
			developmentSchema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLinkAttributes	Grants permission to update a given typed link's attributes. Attributes to be updated must not contribute to the typed link's identity, as defined by its IdentityAttributeOrder	Write	directory*		
UpdateObjectAttributes	Grants permission to update a given object's attributes	Write	directory*		
UpdateSchema	Grants permission to update the schema name with a new name	Write	developmentSchema*		
UpdateTypedLinkFacet	Grants permission to add/update/delete existing Attributes, Rules, identity attribute order of a TypedLinkFacet	Write	developmentSchema*		
UpgradeAppliedSchema	Grants permission to upgrade a single directory in-place using the PublishedSchemaArn with schema updates found in MinorVersion. Backwards-compatible minor version upgrades are instantaneously available for readers on all objects in the directory	Write	directory* publishedSchema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpgradePublishedSchema	Grants permission to upgrade a published schema under a new minor version revision using the current contents of DevelopmentSchemaArn	Write	developmentSchema*		
			publishedSchema*		

Resource types defined by Amazon Cloud Directory

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
appliedSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}/schema/${SchemaName}/${Version}`	
developmentSchema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/development/${SchemaName}`	
directory	`arn:${Partition}:clouddirectory:${Region}:${Account}:directory/${DirectoryId}`	

Resource types	ARN	Condition keys
published Schema	`arn:${Partition}:clouddirectory:${Region}:${Account}:schema/published/${SchemaName}/${Version}`	

Condition keys for Amazon Cloud Directory

Cloud Directory has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Cloud Map

AWS 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 AWS Cloud Map
- Resource types defined by AWS Cloud Map
- Condition keys for AWS Cloud Map

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
CreateService	Grants permission to create a service	Write	namespace*		
			service*		
				servicediscovery:NamespaceArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	Grants permission to delete a specified namespace	Write	namespace*		
DeleteResourcePolicy [permission only]	Grants permission to delete the RAM access control policy for a namespace	Write	namespace*		
DeleteService	Grants permission to delete a specified service	Write	service*		
				servicediscovery:ServiceCreatedByAccount	
DeleteServiceAttributes	Grants permission to delete specified attributes from a service	Write	service*		
				servicediscovery:ServiceCreatedByAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 servicediscovery:ServiceCreatedByAccount	
DiscoverInstances	Grants permission to discover registered instances for a specified namespace and service	Read	namespace*		
			service*		
				servicediscovery:NamespaceName servicediscovery:ServiceName	
DiscoverInstancesRevision	Grants permission to discover the revision of the instances for a specified namespace and service	Read	namespace*		
			service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	Grants permission to get information about a specified instance	Read	service*		
				servicediscovery:ServiceArn	
GetInstancesHealthStatus	Grants permission to get the current health status (Healthy, Unhealthy, or Unknown) of one or more instances	Read	service*		
				servicediscovery:ServiceArn	
GetNamespace	Grants permission to get information about a namespace	Read	namespace*		
GetOperation	Grants permission to get information about a specific operation	Read	namespace*		
			service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy [permission only]	Grants permission to read the RAM access control policy for a namespace	Read	namespace*		
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	service*		
				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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy [permission only]	Grants permission to define the RAM access control policy for a namespace	Write	namespace*		
RegisterInstance	Grants permission to register an instance based on the settings in a specified service	Write	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceCustomHealthStatus	Grants permission to update the current health status for an instance that has a custom health check	Write	service*		
				servicediscovery:ServiceArn servicediscovery:ServiceCreatedByAccount	
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*		
UpdateService	Grants permission to update the settings in a specified service	Write	service*		
				servicediscovery:ServiceCreatedByAccount	
UpdateServiceAttributes	Grants permission to update the attributes in a specified service	Write	service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				servicediscovery:ServiceCreatedByAccount	

Resource types defined by AWS 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 AWS Cloud Map

AWS 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 AWS 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:ServiceCreatedByAccount	Filters access by specifying the account id of the related service creator	String
servicediscovery:ServiceName	Filters access by specifying the name of the related service	String

Actions, resources, and condition keys for AWS Cloud9

AWS Cloud9 (service prefix: `cloud9`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Cloud9

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateEC2Remote [permission only]	Grants permission to start the Amazon EC2 instance that your AWS Cloud9 IDE connects to	Write	environment*		
CreateEnvironmentEC2	Grants permission to create an AWS Cloud9 development environment, launches an Amazon Elastic Compute Cloud (Amazon EC2) instance,	Write		cloud9:EnvironmentName	ec2:DescribeSubnets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	and then hosts the environment on the instance			cloud9:InstanceType cloud9:SubnetId cloud9:UserArn cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateEnvironmentMembership	Grants permission to add an environment member to an AWS Cloud9 development environment	Write	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironmentSSH [permission only]	Grants permission to create an AWS Cloud9 SSH development environment	Write		cloud9:EnvironmentName cloud9:OwnerArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironmentToken [permission only]	Grants permission to create an authentication token that allows a connection between the AWS Cloud9 IDE and the user's environment	Read	environment*		
DeleteEnvironment	Grants permission to delete an AWS Cloud9 development environment. If the environment is hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance, also terminates the instance	Write	environment*		iam:CreateServiceLinkedRole
DeleteEnvironmentMembership	Grants permission to delete an environment member from an AWS Cloud9 development environment	Write	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEC2Remote [permission only]	Grants permission to get details about the connection to the EC2 development environment, including host, user, and port	Read	environment*		
DescribeEnvironmentMemberships	Grants permission to get information about environment members for an AWS Cloud9 development environment	Read	environment*		
				cloud9:UserArn cloud9:EnvironmentId	
DescribeEnvironmentStatus	Grants permission to get status information for an AWS Cloud9 development environment	Read	environment*		
DescribeEnvironments	Grants permission to get information about AWS Cloud9 development environments	Read	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSSHRemote [permission only]	Grants permission to get details about the connection to the SSH development environment, including host, user, and port	Read	environment*		
GetEnvironmentConfig [permission only]	Grants permission to get configuration information that's used to initialize the AWS Cloud9 IDE	Read	environment*		
GetEnvironmentSettings [permission only]	Grants permission to get the AWS Cloud9 IDE settings for a specified development environment	Read	environment*		
GetMembershipSettings [permission only]	Grants permission to get the AWS Cloud9 IDE settings for a specified environment member	Read	environment*		
GetMigrationExperiences [permission only]	Grants permission to get the migration experience for a cloud9 user	Read			
GetUserPublicKey [permission only]	Grants permission to get the user's public SSH key, which is used by AWS Cloud9 to connect to SSH development environments	Read		cloud9:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserSettings [permission only]	Grants permission to get the AWS Cloud9 IDE settings for a specified user	Read			
ListEnvironments	Grants permission to get a list of AWS Cloud9 development environment identifiers	Read			
ListTagsForResource	Grants permission to list tags for a cloud9 environment	Read	environment*		
ModifyTemporaryCredentialsOnEnvironmentEC2 [permission only]	Grants permission to set AWS managed temporary credentials on the Amazon EC2 instance that's used by the AWS Cloud9 integrated development environment (IDE)	Write	environment*		
TagResource	Grants permission to add tags to a cloud9 environment	Tagging	environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a cloud9 environment	Tagging	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateEnvironment	Grants permission to change the settings of an existing AWS Cloud9 development environment	Write	environment*		
UpdateEnvironmentMembership	Grants permission to change the settings of an existing environment member for an AWS Cloud9 development environment	Write	environment*		
				cloud9:UserArn cloud9:EnvironmentId cloud9:Permissions	
UpdateEnvironmentSettings [permission only]	Grants permission to update the AWS Cloud9 IDE settings for a specified development environment	Write	environment*		
UpdateMembershipSettings [permission only]	Grants permission to update the AWS Cloud9 IDE settings for a specified environment member	Write	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSSHRemote [permission only]	Grants permission to update details about the connection to the SSH development environment, including host, user, and port	Write	environment*		
UpdateUserSettings [permission only]	Grants permission to update IDE-specific settings of an AWS Cloud9 user	Write			

Resource types defined by AWS Cloud9

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:${Partition}:cloud9:${Region}:${Account}:environment:${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Cloud9

AWS Cloud9 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
cloud9:EnvironmentId	Filters access by the AWS Cloud9 environment ID	String
cloud9:EnvironmentName	Filters access by the AWS Cloud9 environment name	String
cloud9:InstanceType	Filters access by the instance type of the AWS Cloud9 environment's Amazon EC2 instance	String
cloud9:OwnerArn	Filters access by the owner ARN specified	ARN
cloud9:Permissions	Filters access by the type of AWS Cloud9 permissions	String
cloud9:SubnetId	Filters access by the subnet ID that the AWS Cloud9 environment will be created in	String
cloud9:UserArn	Filters access by the user ARN specified	ARN

Actions, resources, and condition keys for AWS CloudFormation

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateOrganizationsAccess	Grants permission to activate trusted access between StackSets and Organizations. With trusted access between StackSets and Organizations activated, the management account has permissions to create and manage StackSets for your organization	Write			
ActivateType	Grants permission to activate a public third-party extension	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	, making it available for use in stack templates				
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 AWS 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 AWS 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	
DescribeEvents	Grants permission to return all related events for a specified operation	Read	changeset		
			stack		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStackDriftDetectionStatus	Grants permission to return information about a stack drift detection operation	Read			
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, AWS 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 AWS resource descriptions for running and deleted stacks	Read	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStackSet	Grants permission to return the description of the specified stack set	Read	stackset*		
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			
GetHookResult	Grants permission to return detailed information about a specific hook invocation result	Read		cloudformation:TypeArn	kms:Decrypt
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*		
ListAllHookResults	Grants permission to return Hook invocations result information for a specified Hook, a combination of Hook and status, or all Hooks	List		cloudformation:TypeArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChangeSets	Grants permission to return the ID and status of each active change set for a stack. For example, AWS CloudFormation lists change sets that are in the CREATE_IN_PROGRESS or CREATE_PENDING state	List	stack*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag cloudformation resources	Tagging	changeset		
			stack		
			stackset		
				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 AWS 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}	
typeHook	arn:${Partition}:cloudformation:${Region}:${Account}:type/hook/${Type}	
generated template	arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}	
resourcescan	arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}	

Condition keys for AWS CloudFormation

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Condition keys	Description	Type
cloudformation:ChangeSetName	Filters access by an AWS 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 AWS::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 AWS::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
cloudformation:TypeArn	Filters access by the ARN of a CloudFormation extension	ARN

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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for a distribution	Permissions management	distribution		
AssociateAlias	Grants permission to associate an alias to a CloudFront distribution	Write	distribution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDistributionTenantWebACL	Grants permission to associate a distribution tenant with an AWS WAF web ACL	Write	distribution-tenant*		
AssociateDistributionWebACL	Grants permission to associate a distribution with an AWS 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		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	Grants permission to add a new cache policy to CloudFront	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCloudFrontOriginAccessIdentity	Grants permission to create a new CloudFront origin access identity	Write			
CreateConnectionFunction	Grants permission to create a connection function	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectionGroup	Grants permission to create a connection group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContinuousDeploymentPolicy	Grants permission to add a new continuous-deployment policy to CloudFront	Write			
CreateDistribution	Grants permission to create a new web distribution	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudfront:CreateConnectionGroup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDistributionTenant	Grants permission to create a distribution tenant	Write		aws:RequestTag/${TagKey} aws:TagKeys	
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKeyValueStore	Grants permission to create a CloudFront KeyValueStore	Write			
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			
CreatePublicKey	Grants permission to add a new public key to CloudFront	Write			
CreateRealtimeLogConfig	Grants permission to create a real-time log configuration	Write			
CreateResponseHeadersPolicy	Grants permission to add a new response headers policy to CloudFront	Write			
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			
CreateStreamingDistributionWithTags	Grants permission to create a new RTMP distribution with tags	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrustStore	Grants permission to create a trust store	Write		aws:RequestTag/${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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCloudFrontOriginAccessIdentity	Grants permission to delete a CloudFront origin access identity	Write	origin-access-identity*		
DeleteConnectionFunction	Grants permission to delete a connection function	Write	connection-function*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy	Grants permission to delete a resource's policy document	Write	vpcorigin		
DeleteResponseHeadersPolicy	Grants permission to delete a response headers policy	Write	response-headers-policy*		
DeleteStreamingDistribution	Grants permission to delete an RTMP distribution	Write	streaming-distribution*		
DeleteTrustStore	Grants permission to delete a trust store	Write	trust-store*		
DeleteVpcOrigin	Grants permission to delete a VPC origin	Write	vpcorigin*		
DescribeConnectionFunction	Grants permission to get a connection function summary	Read	connection-function*		
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 AWS WAF web ACL	Write	distribution-tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateDistributionWebACL	Grants permission to disassociate a distribution from an AWS 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*		
GetCloudFrontOriginAccessIdentityConfig	Grants permission to get the configuration information about a Cloudfront origin access identity	Read	origin-access-identity*		
GetConnectionFunction	Grants permission to get a connection function's code	Read	connection-function*		
GetConnectionGroup	Grants permission to get information about a connection group	Read	connection-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetResourcePolicy	Grants permission to get the information about a resource's policy document	Read	vpcorigin		
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			
GetStreamingDistribution	Grants permission to get the information about an RTMP distribution	Read	streaming-distribution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStreamingDistributionConfig	Grants permission to get the configuration information about a streaming distribution	Read	streaming-distribution*		
GetTrustStore	Grants permission to get information about a trust store	Read	trust-store*		
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*		
ListConnectionFunctions	Grants permission to list the connection functions in your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConnectionGroups	Grants permission to list the connection groups in your AWS 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 AWS 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 AWS account	List			
ListDistributionsByAnycastIpListId	Grants permission to list the distributions in your account that are associated with the specified AnycastIpListId	List			
ListDistributionsByCachePolicyId	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified cache policy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDistributionsByConnectionFunction	Grants permission to list summaries for distributions associated with the specified connection function	List	connection-function*		
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			
ListDistributionsByTrustStore	Grants permission to list summaries for distributions associated with the specified trust store	List	trust-store*		
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 AWS account with given AWS 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-function		
			connection-group		
			distribution		
			distribution-tenant		
			trust-store		
			vpcorigin		
ListTrustStores	Grants permission to list the trust stores in your AWS account	List			
ListUsages [permission only]	Grants permission to list CloudFront usage	List			
ListVpcOrigins	Grants permission to list VPC origins	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PublishConnectionFunction	Grants permission to publish a connection function	Write	connection-function*		
PublishFunction	Grants permission to publish a CloudFront function	Write	function*		
PutResourcePolicy	Grants permission to update or create a resource's policy document	Write	vpcorigin		
TagResource	Grants permission to add tags to a CloudFront resource	Tagging	anycast-ip-list		
			connection-function		
			connection-group		
			distribution		
			distribution-tenant		
			streaming-distribution		
			trust-store		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestConnectionFunction	Grants permission to test a connection function	Write	connection-function*		
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-function		
			connection-group		
			distribution		
			distribution-tenant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			streaming-distribution		
			trust-store		
			vpcorigin		
				aws:TagKeys	
UpdateAnycastIpList	Grants permission to update an Anycast static IP list	Write	anycast-ip-list*		
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*		
UpdateConnectionFunction	Grants permission to update a connection function	Write	connection-function*		
UpdateConnectionGroup	Grants permission to update a connection group	Write	connection-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateTrustStore	Grants permission to update a trust store	Write	trust-store*		
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}

Resource types	ARN	Condition keys
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}	
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}	

Resource types	ARN	Condition keys
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/${TagKey}
trust-store	arn:${Partition}:cloudfront::${Account}:trust-store/${Id}	aws:ResourceTag/${TagKey}
connection-function	arn:${Partition}:cloudfront::${Account}:connection-function/${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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CloudFront KeyValueStore

Amazon CloudFront KeyValueStore (service prefix: `cloudfront-keyvaluestore`) 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 KeyValueStore
- Resource types defined by Amazon CloudFront KeyValueStore
- Condition keys for Amazon CloudFront KeyValueStore

Actions defined by Amazon CloudFront KeyValueStore

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteKey	Grants permission to delete the key value pair specified by the key	Write	key-value-store*		
DescribeKeyValueStore	Grants permission to return metadata information about Key Value Store	Read	key-value-store*		
GetKey	Grants permission to return a key value pair	Read	key-value-store*		
ListKeys	Grants permission to returns a list of key value pairs	List	key-value-store*		
PutKey	Grants permission to create a new key value pair or replace the value of an existing key	Write	key-value-store*		
UpdateKeys	Grants permission to put or delete multiple key value pairs in a single, all-or-nothing operation	Write	key-value-store*		

Resource types defined by Amazon CloudFront KeyValueStore

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
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${ResourceId}	

Condition keys for Amazon CloudFront KeyValueStore

CloudFront KeyValueStore has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS CloudHSM

AWS CloudHSM (service prefix: cloudhsm) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CloudHSM
- Resource types defined by AWS CloudHSM
- Condition keys for AWS CloudHSM

Actions defined by AWS CloudHSM

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyBackupToRegion	Grants permission to create a copy of a backup in the specified region	Write	backup*		cloudhsm:CopyBackupToRegion cloudhsm:TagResource cloudhsm:UntagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Grants permission to create a new AWS CloudHSM cluster	Write	backup		cloudhsm:TagResource ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:RevokeSecurityGroupEgress iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHsm	Grants permission to create a new hardware security module (HSM) in the specified AWS CloudHSM cluster	Write	cluster*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:RevokeSecurityGroupEgress
DeleteBackup	Grants permission to delete the specified CloudHSM backup	Write	backup*		
DeleteCluster	Grants permission to delete the specified AWS CloudHSM cluster	Write	cluster*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup
DeleteHsm	Grants permission to delete the specified HSM	Write			ec2:DeleteNetworkInterface
DeleteResourcePolicy	Grants permission to delete the policy attached to CloudHSM resources	Write	backup*		
DescribeBackups	Grants permission to get information about backups of AWS CloudHSM clusters	Read			
DescribeClusters	Grants permission to get information about AWS CloudHSM clusters	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy	Grants permission to get information about the policy attached to a AWS CloudHSM resource	Read	backup*		
InitializeCluster	Grants permission to claim an AWS CloudHSM cluster	Write	cluster*		
ListTags	Grants permission to get a list of tags for the specified AWS CloudHSM cluster	Read	backup		
			cluster		
ModifyBackupAttributes	Grants permission to modify attributes for an AWS CloudHSM backup	Write	backup*		
ModifyCluster	Grants permission to modify AWS CloudHSM cluster	Write	cluster*		ec2:DescribeSubnets
PutResourcePolicy	Grants permission to attach a policy to an AWS CloudHSM resource	Write	backup*		
RestoreBackup	Grants permission to restore the specified CloudHSM backup	Write	backup*		
TagResource	Grants permission to add or overwrite one or more tags for the specified AWS CloudHSM cluster	Tagging	backup		
			cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the specified tag or tags from the specified AWS CloudHSM cluster	Tagging	backup		
			cluster		
				aws:TagKeys	

Resource types defined by AWS CloudHSM

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
backup	`arn:${Partition}:cloudhsm:${Region}:${Account}:backup/${CloudHsmBackupInstanceName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
cluster	arn:${Partition}:cloudhsm:${Region}:${Account}:cluster/${CloudHsmClusterInstanceName}	aws:ResourceTag/${TagKey}

Condition keys for AWS CloudHSM

AWS CloudHSM defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CloudSearch

Amazon CloudSearch (service prefix: cloudsearch) 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 CloudSearch

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTags	Attaches resource tags to an Amazon CloudSearch domain	Tagging	domain*		
BuildSuggesters	Indexes the search suggestions	Write	domain*		
CreateDomain	Creates a new search domain	Write	domain*		
DefineAnalysisScheme	Configures an analysis scheme that can be applied to a text or text-array field to define language-specific text processing options	Write	domain*		
DefineExpression	Configures an Expression for the search domain	Write	domain*		
DefineIndexField	Configures an IndexField for the search domain	Write	domain*		
DefineSuggester	Configures a suggester for a domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAnalysisScheme	Deletes an analysis scheme	Write	domain*		
DeleteDomain	Permanently deletes a search domain and all of its data	Write	domain*		
DeleteExpression	Removes an Expression from the search domain	Write	domain*		
DeleteIndexField	Removes an IndexField from the search domain	Write	domain*		
DeleteSuggester	Deletes a suggester	Write	domain*		
DescribeAnalysisSchemes	Gets the analysis schemes configured for a domain	Read	domain*		
DescribeAvailabilityOptions	Gets the availability options configured for a domain	Read	domain*		
DescribeDomainEndpointOptions	Gets the domain endpoint options configured for a domain	Read	domain*		
DescribeDomains	Gets information about the search domains owned by this account	List	domain*		
DescribeExpressions	Gets the expressions configured for the search domain	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIndexFields	Gets information about the index fields configured for the search domain	Read	domain*		
DescribeScalingParameters	Gets the scaling parameters configured for a domain	Read	domain*		
DescribeServiceAccessPolicies	Gets information about the access policies that control access to the domain's document and search endpoints	Read	domain*		
DescribeSuggesters	Gets the suggesters configured for a domain	Read	domain*		
IndexDocuments	Tells the search domain to start indexing its documents using the latest indexing options	Write	domain*		
ListDomainNames	Lists all search domains owned by an account	List	domain*		
ListTags	Displays all of the resource tags for an Amazon CloudSearch domain	Read	domain*		
RemoveTags	Removes the specified resource tags from an Amazon ES domain	Tagging	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAvailabilityOptions	Configures the availability options for a domain	Write	domain*		
UpdateDomainEndpointOptions	Configures the domain endpoint options for a domain	Write	domain*		
UpdateScalingParameters	Configures scaling parameters for a domain	Write	domain*		
UpdateServiceAccessPolicies	Configures the access rules that control access to the domain's document and search endpoints	Permissions management	domain*		
document [permission only]	Allows access to the document service operations	Write	domain		
search [permission only]	Allows access to the search operations	Read	domain		
suggest [permission only]	Allows access to the suggest operations	Read	domain		

Resource types defined by Amazon CloudSearch

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 information about using Amazon CloudSearch resource ARNs in an IAM policy, see Amazon CloudSearch ARNs in the *Amazon CloudSearch Developer Guide*.

Resource types	ARN	Condition keys
domain	`arn:${Partition}:cloudsearch:${Region}:${Account}:domain/${DomainName}`	

Condition keys for Amazon CloudSearch

CloudSearch has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS CloudShell

AWS CloudShell (service prefix: `cloudshell`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CloudShell
- Resource types defined by AWS CloudShell

- Condition keys for AWS CloudShell

Actions defined by AWS CloudShell

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApproveCommand [permission only]	Grants permission to approve a command sent by another AWS service	Read	Environment*		
CreateEnvironment [permission only]	Grants permissions to create a CloudShell environment	Write		cloudshell:SecurityGroupIds cloudshell:SubnetIds cloudshell:VpcIds	
CreateSession [permission only]	Grants permissions to connect to a CloudShell environment from the AWS Management Console	Write	Environment*		
DeleteEnvironment	Grants permission to delete a CloudShell environment	Write	Environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
DescribeEnvironments [permission only]	Grants permission to return descriptions of existing user's environments	List			
GetEnvironmentStatus [permission only]	Grants permission to read a CloudShell environment status	Read	Environment*		
GetFileDownloadUrls [permission only]	Grants permissions to download files from a CloudShell environment	Write	Environment*		
GetFileUploadUrls [permission only]	Grants permissions to upload files to a CloudShell environment	Write	Environment*		
PutCredentials [permission only]	Grants permissions to forward console credentials to the environment	Write	Environment*		
StartEnvironment [permission only]	Grants permission to start a stopped CloudShell environment	Write	Environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEnvironment [permission only]	Grants permission to stop a running CloudShell environment	Write	Environment*		

Resource types defined by AWS CloudShell

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:${Partition}:cloudshell:${Region}:${Account}:environment/${EnvironmentId}`	

Condition keys for AWS CloudShell

AWS CloudShell defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
cloudshell:SecurityGroupIds	Filters access by security group ids. Available during CreateEnvironment operation	ArrayOfString
cloudshell:SubnetIds	Filters access by subnet ids. Available during CreateEnvironment operation	ArrayOfString
cloudshell:VpcIds	Filters access by vpc ids. Available during CreateEnvironment operation	ArrayOfString

Actions, resources, and condition keys for AWS CloudTrail

AWS CloudTrail (service prefix: `cloudtrail`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CloudTrail
- Resource types defined by AWS CloudTrail
- Condition keys for AWS CloudTrail

Actions defined by AWS CloudTrail

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTags	Grants permission to add one or more tags to a trail, event data store, channel or dashboard, up to a limit of 50	Tagging	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/${TagKey} aws:TagKeys	
CancelQuery	Grants permission to cancel a running query	Write	eventdatastore*		
CreateChannel	Grants permission to create a channel	Write	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${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 AWS service	Write	channel*		
CreateTrail	Grants permission to create a trail that specifies the settings for delivery of log data to an Amazon S3 bucket	Write	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization
				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 AWS 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 AWS Glue Data Catalog	Write	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFederation	Grants permission to enable federation of event data store data by using the AWS Glue Data Catalog	Write	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	Grants permission to generate a query for a specified event data store using the CloudTrail Lake query generator	Write	eventdatastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateQueryResultsSummary [permission only]	Grants permission to generate a results summary for specified queries using the CloudTrail natural language generator	Read	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	Grants permission to return information about a specific channel	Read	channel*		
GetDashboard	Grants permission to list settings for the dashboard	Read	dashboard*		
GetEventConfiguration	Grants permission to list event configurations that are configured for a trail or an event data store	Read	eventdatastore		
			trail		
GetEventDataStore	Grants permission to list settings for the event data store	Read	eventdatastore*		
GetEventDataStoreData	Grants permission to get data from an event data store by using the AWS Glue Data Catalog	Read	eventdatastore*		kms:Decrypt kms:GenerateDataKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEventSelectors	Grants permission to list settings for event selectors configured for a trail	Read	trail*		
GetImport	Grants permission to return information about a specific import	Read			
GetInsightSelectors	Grants permission to list CloudTrail Insights selectors that are configured for a trail or event data store	Read	eventdatastore		
			trail		
GetQueryResults	Grants permission to fetch results of a complete query	Read	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy	Grants permission to get the resource policy attached to the provided resource	Read	channel		
			dashboard		
			eventdatastore		
GetServiceLinkedChannel [permission only]	Grants permission to list settings for the service-linked channel	Read	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrail	Grants permission to list settings for the trail	Read	trail*		
GetTrailStatus	Grants permission to retrieve a JSON-formatted list of information about the specified trail	Read	trail*		
ListChannels	Grants permission to list the channels in the current account, and their source names	List			
ListDashboards	Grants permission to list dashboards associated with the current region for your account	List			
ListEventDataStores	Grants permission to list event data stores associated with the current region for your account	List			
ListImportFailures	Grants permission to return a list of failures for the specified import	Read			
ListImports	Grants permission to return information on all imports, or a select set of imports by ImportStatus or Destination	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInsightsData	Grants permission to retrieve data captured by CloudTrail Insights	List	trail*		
ListPublicKeys	Grants permission to list the public keys whose private keys were used to sign trail digest files within a specified time range	Read			
ListQueries	Grants permission to list queries associated with an event data store	List	eventdatastore*		
ListServiceLinkedChannels [permission only]	Grants permission to list service-linked channels associated with the current region for a specified account	List			
ListTags	Grants permission to list the tags for trails, event data stores, channels or dashboards in the current region	Read	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	Grants permission to list trails associated with the current region for your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LookupEvents	Grants permission to look up and retrieve metric data for API activity events captured by CloudTrail that create, update, or delete resources in your account	Read			
PutEventConfiguration	Grants permission to create and update event configurations for a trail or an event data store	Write	eventdatastore		iam:CreateServiceLinkedRole iam:GetRole
			trail		
PutEventSelectors	Grants permission to create and update event selectors for a trail	Write	trail*		
PutInsightSelectors	Grants permission to create and update CloudTrail Insights selectors for a trail or event data store	Write	eventdatastore		
			trail		
PutResourcePolicy	Grants permission to attach a resource policy to the provided resource	Write	channel		
			dashboard		
			eventdatastore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterOrganizationDelegatedAdmin	Grants permission to register an AWS Organizations member account as a delegated administrator	Write			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator
RemoveTags	Grants permission to remove tags from a trail, event data store, channel or dashboard	Tagging	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:TagKeys	
RestoreEventDataStore	Grants permission to restore an event data store	Write	eventdatastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchSampleQueries	Grants permission to perform semantic search for CloudTrail Lake sample queries	Read			
StartDashboardRefresh	Grants permission to start a refresh on the specified dashboard	Write	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	Grants permission to start ingestion on an event data store	Write	eventdatastore*		
StartImport	Grants permission to start an import of logged trail events from a source S3 bucket to a destination event data store	Write			
StartLogging	Grants permission to start the recording of AWS API calls and log file delivery for a trail	Write	trail*		
StartQuery	Grants permission to start a new query on a specified event data store	Write	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	Grants permission to stop ingestion on an event data store	Write	eventdatastore*		
StopImport	Grants permission to stop a specified import	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopLogging	Grants permission to stop the recording of AWS API calls and log file delivery for a trail	Write	trail*		
UpdateChannel	Grants permission to update a channel	Write	channel*		
UpdateDashboard	Grants permission to update a dashboard	Write	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEventDataStore	Grants permission to update an event data store	Write	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
UpdateServiceLinkedChannel [permission only]	Grants permission to update the service-linked channel settings for delivery of log data to an AWS service	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTrail	Grants permission to update the settings that specify delivery of log files	Write	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Resource types defined by AWS CloudTrail

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

> **Note**
>
> For policies that control access to CloudTrail actions, the Resource element is always set to "*". For information about using resource ARNs in an IAM policy, see How AWS CloudTrail works with IAM in the *AWS CloudTrail User Guide*.

Resource types	ARN	Condition keys
trail	arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}	aws:ResourceTag/${TagKey}
eventdatastore	arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/${EventDataStoreId}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}

Condition keys for AWS CloudTrail

AWS CloudTrail defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to the resource	String
aws:TagKeys	Filters access by the tag keys in a request	ArrayOfString

Actions, resources, and condition keys for AWS CloudTrail Data

AWS CloudTrail Data (service prefix: `cloudtrail-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 AWS CloudTrail Data

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAuditEvents	Grants permission to ingest your application events into CloudTrail Lake	Write	channel*		

Resource types defined by AWS CloudTrail Data

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types

that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

> **Note**
>
> For policies that control access to CloudTrail actions, the Resource element is always set to "*". For information about using resource ARNs in an IAM policy, see How AWS CloudTrail works with IAM in the *AWS CloudTrail User Guide*.

Resource types	ARN	Condition keys
channel	`arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS CloudTrail Data

AWS CloudTrail Data defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag's key and value in a request	String
aws:ResourceTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetServiceLevelIndicatorReport	Grants permission to batch get service level indicator report	Read			
BatchGetServiceLevelObjectiveBudgetReport	Grants permission to batch retrieve a service level objective budget report	Read	slo*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServiceLevelObjective	Grants permission to create a service level objective	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmMuteRule	Grants permission to delete an alarm mute rule	Write	alarm-mute-rule*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableInsightRules	Grants permission to enable a collection of insight rules	Write	insight-rule*		
EnableTopologyDiscovery	Grants permission to enable a CloudWatch topology discovery	Write			
GenerateQuery	Grants permission to generate a Metrics Insights or Logs Insights query string from a natural language prompt	Read			
GenerateQueryResultsSummary	Grants permission to generate a summary of CloudWatch LogInsights query results in natural language using generative AI	Read			
GetAlarmMuteRule	Grants permission to get an alarm mute rule	Read	alarm-mute-rule*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTopologyMap	Grants permission to retrieve a CloudWatch topology map	Read			
Link [permission only]	Grants permission to share CloudWatch resources with a monitoring account	Write			
ListAlarmMuteRules	Grants permission to retrieve a list of alarm mute rules owned by the user's account	List	alarm-mute-rule*		
ListDashboards	Grants permission to return a list of all CloudWatch dashboards in your account	List			
ListEntitiesForMetric [permission only]	Grants permission to retrieve all the entities that are emitting a given metric	List			
ListManagedInsightRules	Grants permission to list available managed Insight Rules for a given Resource ARN	Read		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMetricStreams	Grants permission to return a list of all CloudWatch metric streams in your account	List			
ListMetrics	Grants permission to retrieve a list of valid metrics stored for the AWS account owner	List			
ListServiceLevelObjectives	Grants permission to list service level objectives	List			
ListServices	Grants permission to list services	List			
ListTagsForResource	Grants permission to list tags for an Amazon CloudWatch resource	List	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-AlarmMuteRule		alarm-mute-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		
PutAlarmMuteRule	Grants permission to create or update an alarm mute rule	Write	alarm-mute-rule*		
			alarm		
				aws:RequestTag/${TagKey} aws:TagKeys	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	Grants permission to create a CloudWatch dashboard, or update an existing dashboard if it already exists	Write	dashboard*		
PutInsightRule	Grants permission to create a new insight rule or replace an existing insight rule	Write	insight-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutManagedInsightRules	Grants permission to create managed Insight Rules	Write		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
PutMetricAlarm	Grants permission to create or update an alarm and associates it with the specified Amazon CloudWatch metric	Write	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	Grants permission to publish metric data points to Amazon CloudWatch	Write		cloudwatch:namespace	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
StartMetricStreams	Grants permission to start all CloudWatch metric streams that you specify	Write	metric-stream*		
StopMetricStreams	Grants permission to stop all CloudWatch metric streams that you specify	Write	metric-stream*		
TagResource	Grants permission to add tags to an Amazon CloudWatch resource	Tagging	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-AlarmMuteRule		alarm-mute-rule*		
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Grants permission to remove a tag from an Amazon CloudWatch resource	Tagging	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-AlarmMuteRule		alarm-mute-rule*		
	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}

Resource types	ARN	Condition keys
alarm-mute-rule	arn:${Partition}:cloudwatch:${Region}:${Account}:alarm-mute-rule:${AlarmMuteRuleName}	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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value associated with the resource	String
aws:TagKeys	Filters actions based on the presence of mandatory tags in the request	ArrayOfString
cloudwatch:AlarmActions	Filters actions based on defined alarm actions	ArrayOfString
cloudwatch:namespace	Filters actions based on the presence of optional namespace values	String
cloudwatch: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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteComponent	Grants permission to delete a component	Write			
DeleteLogPattern	Grants permission to delete a log pattern	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWorkload	Grants permission to describe a workload	Read			
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals (service prefix: `application-signals`) 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 Signals

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetServiceLevelObjectiveBudgetReport	Grants permission to batch retrieve a service level objective budget report	Read	slo*		
BatchUpdateExclusionWindows	Grants permission to add or remove exclusion windows from Amazon CloudWatch SLOs	Write	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	
DeleteGroupingConfiguration	Grants permission to delete a grouping configuration	Write			
DeleteServiceLevelObjective	Grants permission to delete a service level objective	Write	slo*		
GetService	Grants permission to retrieve information about a service	Read			
GetServiceLevelObjective	Grants permission to retrieve information about service level objective	Read	slo*		
Link [permission only]	Grants permission to share Application Signals resources with a monitoring account	Write			
ListAuditFindings	Grants permission to list service auditing results	List			
ListEntityEvents	Grants permission to list events for an entity	List			
ListGroupingAttributeDefinitions	Grants permission to list grouping attribute configurations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListObservedEntities	Grants permission to list entities associated with other entities	List			
ListServiceDependencies	Grants permission to list service dependencies	Read			
ListServiceDependents	Grants permission to list service dependents	Read			
ListServiceLevelObjectiveExclusionWindows	Grants permission to list exclusion windows for an Amazon CloudWatch SLO	List	slo*		
ListServiceLevelObjectives	Grants permission to list service level objectives	List			
ListServiceOperations	Grants permission to list service operations	Read			
ListServiceStates	Grants permission to list service states	List			
ListServices	Grants permission to list services	List			
ListTagsForResource	Grants permission to list tags for an Amazon CloudWatch SLO	Read	slo*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutGroupingConfiguration	Grants permission to create or update a grouping configuration	Write			
StartDiscovery	Grants permission to enable CloudWatch discovery	Write			
TagResource	Grants permission to add tags to an Amazon CloudWatch SLO	Tagging	slo*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag to an Amazon CloudWatch SLO	Tagging	slo*		
				aws:TagKeys	
UpdateServiceLevelObjective	Grants permission to update a service level objective	Write	slo*		

Resource types defined by Amazon CloudWatch Application Signals

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
slo	arn:${Partition}:application-signals:${Region}:${Account}:slo/${SloName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Application Signals

Amazon CloudWatch Application Signals defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CloudWatch Evidently

Amazon CloudWatch Evidently (service prefix: evidently) 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 Evidently

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchEvaluateFeature	Grants permission to send a batched evaluate feature request	Write	Feature*		
CreateExperiment	Grants permission to create an experiment	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeature	Grants permission to create a feature	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateLaunch	Grants permission to create a launch	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Grants permission to create a project	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:GetRole
CreateSegment	Grants permission to create a segment	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteExperiment	Grants permission to delete an experiment	Write	Experiment*		
DeleteFeature	Grants permission to delete a feature	Write	Feature*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLaunch	Grants permission to delete a launch	Write	Launch*		
DeleteProject	Grants permission to delete a project	Write	Project*		
DeleteSegment	Grants permission to delete a segment	Write	Segment*		
EvaluateFeature	Grants permission to send an evaluate feature request	Write	Feature*		
GetExperiment	Grants permission to get experiment details	Read	Experiment*		
GetExperimentResults	Grants permission to get experiment result	Read	Experiment*		
GetFeature	Grants permission to get feature details	Read	Feature*		
GetLaunch	Grants permission to get launch details	Read	Launch*		
GetProject	Grants permission to get project details	Read	Project*		
GetSegment	Grants permission to get segment details	Read	Segment*		
ListExperiments	Grants permission to list experiments	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFeatures	Grants permission to list features	Read			
ListLaunches	Grants permission to list launches	Read			
ListProjects	Grants permission to list projects	Read			
ListSegmentReferences	Grants permission to list resources referencing a segment	Read			
ListSegments	Grants permission to list segments	Read			
ListTagsForResource	Grants permission to list tags for resources	Read			
PutProjectEvents	Grants permission to send performance events	Write	Project*		
StartExperiment	Grants permission to start an experiment	Write	Experiment*		
StartLaunch	Grants permission to start a launch	Write	Launch*		
StopExperiment	Grants permission to stop an experiment	Write	Experiment*		
StopLaunch	Grants permission to stop a launch	Write	Launch*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag resources	Tagging	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestSegmentPattern	Grants permission to test a segment pattern	Read			
UntagResource	Grants permission to untag resources	Tagging	Experiment		
			Feature		
			Launch		
			Project		
			Segment		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExperiment	Grants permission to update experiment	Write	Experiment*		
UpdateFeature	Grants permission to update feature	Write	Feature*		
UpdateLaunch	Grants permission to update a launch	Write	Launch*		
UpdateProject	Grants permission to update project	Write	Project*		iam:CreateServiceLinkedRole iam:GetRole
UpdateProjectDataDelivery	Grants permission to update project data delivery	Write	Project*		

Resource types defined by Amazon CloudWatch Evidently

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:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}	aws:ResourceTag/${TagKey}
Feature	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/feature/${FeatureName}	aws:ResourceTag/${TagKey}
Experiment	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/experiment/${ExperimentName}	aws:ResourceTag/${TagKey}
Launch	arn:${Partition}:evidently:${Region}:${Account}:project/${ProjectName}/launch/${LaunchName}	aws:ResourceTag/${TagKey}
Segment	arn:${Partition}:evidently:${Region}:${Account}:segment/${SegmentName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Evidently

Amazon CloudWatch Evidently defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed the request on behalf of the IAM principal	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource that make the request on behalf of the IAM principal	String
aws:TagKeys	Filters access by the tag keys that are passed in the request on behalf of the IAM principal	ArrayOfString

Actions, resources, and condition keys for Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor (service prefix: `internetmonitor`) 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 Internet Monitor
- Resource types defined by Amazon CloudWatch Internet Monitor
- Condition keys for Amazon CloudWatch Internet Monitor

Actions defined by Amazon CloudWatch Internet Monitor

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMonitor	Grants permission to create a monitor	Write	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteMonitor	Grants permission to delete a monitor	Write	Monitor*		
GetHealthEvent	Grants permission to get information about a health event for a specified monitor	Read	Monitor*		
GetInternetEvent	Grants permission to get information about a specified internet event	Read	InternetEvent*		
GetMonitor	Grants permission to get information about a monitor	Read	Monitor*		
GetQueryResults	Grants permission to get results for a data query for a monitor	Read	Monitor*		
GetQueryStatus	Grants permission to get status for a data query for a monitor	Read	Monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Link [permission only]	Grants permission to share Internet Monitor resources with a monitoring account	Write			
ListHealthEvents	Grants permission to list all health events for a monitor	List	Monitor*		
ListInternetEvents	Grants permission to list all internet events	List			
ListMonitors	Grants permission to list all monitors in an account and their statuses	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	Monitor*		
StartQuery	Grants permission to start a data query for a monitor	Read	Monitor*		
StopQuery	Grants permission to stop a data query for a monitor	Read	Monitor*		
TagResource	Grants permission to add tags to a resource	Tagging	Monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	Monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateMonitor	Grants permission to update a monitor	Write	Monitor*		

Resource types defined by Amazon CloudWatch Internet Monitor

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
HealthEvent	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}/health-event/${EventId}`	aws:ResourceTag/${TagKey}
Monitor	`arn:${Partition}:internetmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
InternetEvent	`arn:${Partition}:internetmonitor::${Account}:internet-event/${InternetEventId}`	

Condition keys for Amazon CloudWatch Internet Monitor

Amazon CloudWatch Internet Monitor defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag key-value pairs in the request	String
aws:ResourceTag/${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 CloudWatch Logs

Amazon CloudWatch Logs (service prefix: `logs`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon CloudWatch Logs
- Resource types defined by Amazon CloudWatch Logs
- Condition keys for Amazon CloudWatch Logs

Actions defined by Amazon CloudWatch Logs

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateKmsKey	Grants permission to associate the specified AWS Key Management Service (AWS KMS) customer master key (CMK) with the specified log group	Write	log-group*		
AssociateSourceToS3TableIntegration	Grants permission to associate a log source to an S3 Tables integration	Write			
CallWithBearerToken [permission only]	Grants permission to authenticate requests using bearer token	Write			
CancelExportTask	Grants permission to cancel an export task if it is in PENDING or RUNNING state	Write			
CancelImportTask	Grants permission to cancel an import from CloudTrail Lake to CloudWatch	Write			
CreateDelivery	Grants permission to create a delivery connecting a delivery	Write	delivery*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	source to a delivery destination		delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportTask	Grants permission to create an ExportTask which allows you to efficiently export data from a Log Group to your Amazon S3 bucket	Write	log-group*		
CreateImportTask	Grants permission to start an asynchronous process to import data from a CloudTrail Lake event data store into a managed log group in CloudWatch	Write			
CreateLogAnomalyDetector	Grants permission to create a log anomaly detector	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}	
CreateLogStream	Grants permission to create a new log stream with the specified name	Write	log-stream*		
CreateScheduledQuery	Grants permission to create a scheduled query	Write	scheduled-query*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccountPolicy	Grants permission to delete an account policy	Write			
DeleteDataProtectionPolicy	Grants permission to delete a data protection policy attached to a log group	Write	log-group*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDestination	Grants permission to delete the destination with the specified name	Write	destination*		
DeleteIndexPolicy	Grants permission to delete an index policy attached to a log group	Write			
DeleteIntegration	Grants permission to delete the integration	Write			
DeleteLogAnomalyDetector	Grants permission to delete a log anomaly detector	Write	anomaly-detector*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePipelineRule [permission only]	Grants permission to delete telemetry pipeline	Write			
DeleteQueryDefinition	Grants permission to delete a saved CloudWatch Logs Insights query definition	Write			
DeleteResourcePolicy	Grants permission to delete a resource policy from this account	Permissions management			
DeleteRetentionPolicy	Grants permission to delete the retention policy of the specified log group	Write	log-group*		
DeleteScheduledQuery	Grants permission to delete a scheduled query	Write	scheduled-query*		
DeleteSubscriptionFilter	Grants permission to delete a subscription filter associated with the specified log group	Write	log-group*		
DeleteTransformer	Grants permission to delete a transformer associated with the specified log group	Write	log-group*		
DescribeAccountPolicies	Grants permission to retrieve account policies	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConfigurationTemplates	Grants permission to retrieve a list of configuration templates of available log types	List			
DescribeDeliveries	Grants permission to retrieve a list of deliveries an account	List			
DescribeDeliveryDestinations	Grants permission to retrieve a list of delivery destinations an account	List			
DescribeDeliverySources	Grants permission to retrieve a list of delivery sources in an account	List			
DescribeDestinations	Grants permission to return all the destinations that are associated with the AWS account making the request	List			
DescribeExportTasks	Grants permission to return all the export tasks that are associated with the AWS account making the request	List			
DescribeFieldIndexes	Grants permission to return all the indexing attributes that are attached with the log groups	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImportTaskBatches	Grants permission to return detailed information about the individual batches within an import task, including status and any error	List			
DescribeImportTasks	Grants permission to return all the import tasks associated with the AWS account making the request	List			
DescribeIndexPolicies	Grants permission to return all the index policies that are attached with the log groups	List			
DescribeLogGroups	Grants permission to return all the log groups that are associated with the AWS account making the request	List			
DescribeLogStreams	Grants permission to return all the log streams that are associated with the specified log group	List	log-group*		
DescribeMetricFilters	Grants permission to return all the metrics filters associated with the specified log group	List	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DisassociateKmsKey	Grants permission to disassociate the associated AWS Key Management Service (AWS KMS) customer master key (CMK) from the specified log group	Write	log-group*		
DisassociateSourceFromS3TableIntegration	Grants permission to disassociate a log source from an S3 Tables integration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLogEvents	Grants permission to retrieve log events from the specified log stream	Read	log-stream*		
GetLogFields	Grants permission to retrieve a list of log fields for a data source	Read			
GetLogGroupFields	Grants permission to return a list of the fields that are included in log events in the specified log group, along with the percentage of log events that contain each field	Read	log-group*		
GetLogRecord	Grants permission to retrieve all the fields and values of a single log event	Read	log-group*		
GetQueryResults	Grants permission to return the results from the specified query	Read	log-group*		
GetScheduledQuery	Grants permission to retrieve information about a specified scheduled query	Read	scheduled-query*		
GetScheduledQueryHistory	Grants permission to return the execution history for a specified scheduled query	Read	scheduled-query*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransformer	Grants permission to return transformer associated with the specified log group	Read	log-group*		
IntegrateWithS3Table [permission only]	Grants permission to deliver log events to S3 Tables	Write	log-group*		
Link [permission only]	Grants permission to share CloudWatch resources with a monitoring account	Write			
ListAggregateLogGroupSummaries	Grants permission to return an aggregate summary of all log groups in the region grouped by specified data-source characteristics	List			
ListAnomalies	Grants permission to list all anomalies detected in the AWS account making the request	List	anomaly-detector		
ListEntitiesForLogGroup [permission only]	Grants permission to retrieve all the entities that are associated with log group	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIntegrations	Grants permission to list all integrations associated with the AWS account making the request	List			
ListLogAnomalyDetectors	Grants permission to return all the anomaly detectors that are associated with the AWS account making the request	List	anomaly-detector		
ListLogDeliveries [permission only]	Grants permission to list all the log deliveries for specified account and/or log source	List			
ListLogGroups	Grants permission to return all the log groups that are associated with the AWS account making the request	List			
ListLogGroupsForEntity [permission only]	Grants permission to retrieve all the log groups that are associated with entity	List			
ListLogGroupsForQuery	Grants permission to return all the log groups that are associated with the specified query	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListScheduledQueries	Grants permission to return all scheduled queries that are associated with the AWS account making the request	List			
ListSourcesForS3TableIntegration	Grants permission to return all log sources associated with an S3 Tables integration	List			
ListTagsForResource	Grants permission to list the tags for the specified resource	List	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	Grants permission to list the tags for the specified log group	List	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ProcessWithPipeline [permission only]	Grants permission to process and transform log events through pipeline transformers before storage	Write	log-group*		
PutAccountPolicy	Grants permission to attach an account policy	Write			
PutBearerTokenAuthentication	Grants permission to enable or disable bearer token based authentication for the specified log group	Write	log-group*		
PutDataProtectionPolicy	Grants permission to attach a data protection policy to detect and redact sensitive information from log events	Write	log-group*		
PutDeliveryDestination	Grants permission to create/update a delivery destination	Write	delivery-destination*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	Grants permission to attach a delivery destination policy to a delivery destination	Write	delivery-destination*		
PutDeliverySource	Grants permission to create/update a delivery source	Write	delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDestination	Grants permission to create or update a Destination	Write	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	Grants permission to create or update an access policy associated with an existing Destination	Write	destination*		
PutIndexPolicy	Grants permission to attach an index policy at log group level to optimize search and query	Write			
PutIntegration	Grants permission to create integration between cloudwatch logs and opensearch	Write			
PutLogEvents	Grants permission to upload a batch of log events to the specified log stream	Write	log-stream*		
PutLogGroupDeletionProtection	Grants permission to enable or disable deletion protection for the specified log group	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricFilter	Grants permission to create or update a metric filter and associates it with the specified log group	Write	log-group*		
PutPipelineRule [permission only]	Grants permission to create telemetry pipeline	Write			
PutQueryDefinition	Grants permission to create or update a query definition	Write			
PutResourcePolicy	Grants permission to create or update a resource policy allowing other AWS services to put log events to this account	Permissions management			
PutRetentionPolicy	Grants permission to set the retention of the specified log group	Write	log-group*		
PutSubscriptionFilter	Grants permission to create or update a subscription filter and associates it with the specified log group	Write	log-group*		iam:PassRole
			destination		
PutTransformer	Grants permission to create or update a transformer and associates it with the specified log group	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartLiveTail	Grants permission to start a Live Tail session in CloudWatch Logs	Read	log-group*		
StartQuery	Grants permission to schedule a query of a log group using CloudWatch Logs Insights	Read	log-group*		
StopLiveTail [permission only]	Grants permission to stop a Live Tail session that is in progress	Read			
StopQuery	Grants permission to stop a CloudWatch Logs Insights query that is in progress	Read			
TagLogGroup	Grants permission to add or update the specified tags for the specified log group	Tagging	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Grants permission to add or update the specified tags for the specified resource	Tagging	anomaly-detector		
			delivery		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			delivery-destination		
			delivery-source		
			destination		
			log-group		
			scheduled-query		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	Grants permission to test the filter pattern of a metric filter against a sample of log event messages	Read			
TestTransformer	Grants permission to test the transformer against a sample of log event messages	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Unmask [permission only]	Grants permission to fetch unmasked log events that have been redacted with a data protection policy	Read	log-group*		
UntagLogGroup	Grants permission to remove the specified tags from the specified log group	Tagging	log-group*		
				aws:TagKeys	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
			scheduled-query		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAnomaly	Grants permission to update an anomaly reported by a log anomaly detector	Write	anomaly-detector*		
UpdateDeliveryConfiguration	Grants permission to update configuration related to a delivery	Write	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateLogAnomalyDetector	Grants permission to update a log anomaly detector	Write	anomaly-detector*		
UpdateLogDelivery [permission only]	Grants permission to update the log delivery information for specified log delivery	Write			
UpdateScheduledQuery	Grants permission to update a scheduled query	Write	scheduled-query*		

Resource types defined by Amazon CloudWatch Logs

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
log-group	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}`	aws:ResourceTag/${TagKey}
log-stream	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}`	aws:ResourceTag/${TagKey}
destination	`arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}`	aws:ResourceTag/${TagKey}
delivery-source	`arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}`	aws:ResourceTag/${TagKey}
delivery	`arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}`	aws:ResourceTag/${TagKey}
delivery-destination	`arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}`	aws:ResourceTag/${TagKey}
anomaly-detector	`arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
scheduled-query	arn:${Partition}:logs:${Region}:${Account}:scheduled-query:${ScheduledQueryId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Logs

Amazon CloudWatch Logs defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
logs:DeliveryDestinationResourceArn	Filters access by the Log Destination ARN passed in the request	ARN
logs:LogGeneratingResourceArns	Filters access by the Log Generating Resource ARNs passed in the request	ArrayOfARN

Actions, resources, and condition keys for Amazon CloudWatch Network Synthetic Monitor

Amazon CloudWatch Network Synthetic Monitor (service prefix: `networkmonitor`) 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 Network Synthetic Monitor

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMonitor	Grants permission to create a monitor	Write	monitor*		
CreateProbe	Grants permission to create a probe	Write			
DeleteMonitor	Grants permission to delete a monitor	Write	monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProbe	Grants permission to delete a probe	Write	probe*		
GetMonitor	Grants permission to get information about a monitor	Read	monitor*		
GetProbe	Grants permission to get information about a probe	Read	probe*		
ListMonitors	Grants permission to list all monitors in an account and their statuses	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	monitor		
			probe		
TagResource	Grants permission to add tags to a resource	Tagging	monitor		
			probe		
UntagResource	Grants permission to remove tags from a resource	Tagging	monitor		
			probe		
				aws:TagKeys	
UpdateMonitor	Grants permission to update a monitor	Write	monitor*		
UpdateProbe	Grants permission to update a probe	Write	probe*		

Resource types defined by Amazon CloudWatch Network Synthetic Monitor

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
monitor	`arn:${Partition}:networkmonitor:${Region}:${Account}:monitor/${MonitorName}`	aws:ResourceTag/${TagKey}
probe	`arn:${Partition}:networkmonitor:${Region}:${Account}:probe/${ProbeId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Network Synthetic Monitor

Amazon CloudWatch Network Synthetic Monitor defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys in the request	ArrayOfString

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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	Grants permission to delete a link between a monitoring account and a source account for cross-account monitoring	Write	Link*		
				aws:ResourceTag/${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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutSinkPolicy	Grants permission to create or update the IAM policy for a cross-account monitoring sink	Write	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a resource	Tagging	Link		
			Sink		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	Link		
			Sink		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
oam:ResourceTypes	Filters access by the presence of resource types in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CloudWatch Observability Admin Service

Amazon CloudWatch Observability Admin Service (service prefix: `observabilityadmin`) 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 Admin Service
- Resource types defined by Amazon CloudWatch Observability Admin Service
- Condition keys for Amazon CloudWatch Observability Admin Service

Actions defined by Amazon CloudWatch Observability Admin Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCentralizationRuleForOrganization	Grants permission to create a new organization centralization rule with the specified name for the organization	Write	organization-centralization-rule*		
				aws:TagKeys aws:RequestTag/${TagKey} observabilityadmin:CentralizationSourceRegions observabilityadmin:CentralizationDestinationRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				observabilityadmin:CentralizationBackupRegion	
CreateS3TableIntegration	Grants permission to create a new s3 table integration with the specified configuration	Write	s3tableintegration *		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTelemetryPipeline	Grants permission to create a new telemetry pipeline with the specified name and configuration	Write	telemetry-pipeline *		
				aws:TagKeys aws:RequestTag/${TagKey} observabilityadmin:SourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTelemetryRule	Grants permission to create a new telemetry rule with the specified name for the account	Write	telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTelemetryRuleForOrganization	Grants permission to create a new organization telemetry rule with the specified name for the organization	Write	organization-telemetry-rule*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCentralizationRuleForOrganization	Grants permission to delete an organization centralization rule with the specified name for the organization	Write	organization-centralization-rule*		
DeleteS3TableIntegration	Grants permission to delete the s3 table integration with the specified arn	Write	s3tableintegration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTelemetryPipeline	Grants permission to delete the telemetry pipeline with the specified arn	Write	telemetry-pipeline*		
DeleteTelemetryRule	Grants permission to delete a telemetry rule with the specified name for the account	Write	telemetry-rule*		
DeleteTelemetryRuleForOrganization	Grants permission to delete an organization telemetry rule with the specified name for the organization	Write	organization-telemetry-rule*		
GetCentralizationRuleForOrganization	Grants permission to retrieve the specified organization centralization rule for the organization	Read	organization-centralization-rule*		
GetS3TableIntegration	Grants permission to retrieve the specified s3 table integration for the account	Read	s3tableintegration*		
GetTelemetryEnrichmentStatus	Grants permission to retrieve the status of the Resource tags for telemetry feature for the account	Read			
GetTelemetryEvaluationStatus	Grants permission to retrieve the Telemetry Config feature status for the account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTelemetryEvaluationStatusForOrganization	Grants permission to retrieve the Telemetry Config feature status for the organization	Read			
GetTelemetryPipeline	Grants permission to Get the telemetry pipeline with the specified name or arn	Read	telemetry-pipeline*		
GetTelemetryRule	Grants permission to retrieve the specified telemetry rule for the account	Read	telemetry-rule*		
GetTelemetryRuleForOrganization	Grants permission to retrieve the specified organization telemetry rule for the organization	Read	organization-telemetry-rule*		
ListCentralizationRulesForOrganization	Grants permission to list the centralization rules for the organization	List			
ListResourceTelemetry	Grants permission to retrieve telemetry configurations for resources associated with the account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceTelemetryForOrganization	Grants permission to retrieve telemetry configurations for resources associated with accounts in the organization	Read			
ListS3TableIntegrations	Grants permission to list s3 table integrations for the account	List			
ListTagsForResource	Grants permission to list the tags for the specified resource	List	organization-centralization-rule		
			organization-telemetry-rule		
			s3tableintegration		
			telemetry-pipeline		
			telemetry-rule		
ListTelemetryPipelines	Grants permission to List telemetry pipelines for the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTelemetryRules	Grants permission to list the telemetry rules for the account	List			
ListTelemetryRulesForOrganization	Grants permission to list the telemetry rules for the organization	List			
StartTelemetryEnrichment	Grants permission to enable the Resource tags for telemetry feature for the account	Write			
StartTelemetryEvaluation	Grants permission to start the Telemetry Config feature for the account	Write			
StartTelemetryEvaluationForOrganization	Grants permission to start the Telemetry Config feature for the organization	Write			
StopTelemetryEnrichment	Grants permission to disable the Resource tags for telemetry feature for the account	Write			
StopTelemetryEvaluation	Grants permission to stop the Telemetry Config feature for the account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopTelemetryEvaluationForOrganization	Grants permission to stop the Telemetry Config feature for the organization	Write			
TagResource	Grants permission to add or update the specified tags for the specified resource	Tagging	organization-centralization-rule		
			organization-telemetry-rule		
			s3tableintegration		
			telemetry-pipeline		
			telemetry-rule		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestTelemetryPipeline	Grants permission to Test a telemetry pipeline configuration with sample data	Read			
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	organization-centralization-rule		
			organization-telemetry-rule		
			s3tableintegration		
			telemetry-pipeline		
			telemetry-rule		
				aws:TagKeys	
UpdateCentralizationRuleForOrganization	Grants permission to update the specified centralization rule for the organization	Write	organization-centralization-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				observabilityadmin:CentralizationSourceRegions observabilityadmin:CentralizationDestinationRegion observabilityadmin:CentralizationBackupRegion	
UpdateTelemetryPipeline	Grants permission to Update the telemetry pipeline with the specified arn	Write	telemetry-pipeline*		
UpdateTelemetryRule	Grants permission to update the specified telemetry rule for the account	Write	telemetry-rule*		
UpdateTelemetryRuleForOrganization	Grants permission to update the specified telemetry rule for the organization	Write	organization-telemetry-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateTelemetryPipelineConfiguration	Grants permission to Validate a telemetry pipeline configuration	Read			

Resource types defined by Amazon CloudWatch Observability Admin 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
telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:telemetry-rule/${TelemetryRuleName}`	aws:ResourceTag/${TagKey}
organization-telemetry-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:organization-telemetry-rule/${TelemetryRuleName}`	aws:ResourceTag/${TagKey}
organization-centralization-rule	`arn:${Partition}:observabilityadmin:${Region}:${Account}:organization-centralization-rule/${CentralizationRuleName}`	aws:ResourceTag/${TagKey}
telemetry-pipeline	`arn:${Partition}:observabilityadmin:${Region}:${Account}:telemetry-pipeline/${TelemetryPipelineIdentifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
s3tableintegration	arn:${Partition}:observabilityadmin:${Region}:${Account}:s3tableintegration/${S3TableIntegrationIdentifier}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Observability Admin Service

Amazon CloudWatch Observability Admin Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
observabilityadmin:CentralizationBackupRegion	Filters access by the backup region that is passed in the request	String
observabilityadmin:Centrali	Filters access by the destination region that is passed in the request	String

Condition keys	Description	Type
zationDestinationRegion		
observabilityadmin:CentralizationSourceRegions	Filters access by the source regions that are passed in the request	ArrayOfString
observabilityadmin:SourceType	Filters access by the source type that is passed in the request	String

Actions, resources, and condition keys for AWS CloudWatch RUM

AWS CloudWatch RUM (service prefix: `rum`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CloudWatch RUM
- Resource types defined by AWS CloudWatch RUM
- Condition keys for AWS CloudWatch RUM

Actions defined by AWS CloudWatch RUM

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateRumMetricDefinitions	Grants permission to create rum metric definitions	Write	AppMonitorResource*		
BatchDeleteRumMetricDefinitions	Grants permission to remove rum metric definitions	Write	AppMonitorResource*		
BatchGetRumMetricDefinitions	Grants permission to get rum metric definitions	Read	AppMonitorResource*		
CreateAppMonitor	Grants permission to create appMonitor metadata	Write	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAppMonitor	Grants permission to delete appMonitor metadata	Write	AppMonitorResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy	Grants permission to delete a resource policy attached to an app monitor	Write	AppMonitorResource*		
DeleteRumMetricsDestination	Grants permission to delete rum metrics destinations	Write	AppMonitorResource*		
GetAppMonitor	Grants permission to get appMonitor metadata	Read	AppMonitorResource*		
GetAppMonitorData	Grants permission to get appMonitor data	Read	AppMonitorResource*		
GetResourcePolicy	Grants permission to retrieve a resource policy attached to an app monitor	Read	AppMonitorResource*		
ListAppMonitors	Grants permission to list appMonitors metadata	List			
ListRumMetricsDestinations	Grants permission to list rum metrics destinations	Read	AppMonitorResource*		
ListTagsForResource	Grants permission to list tags for resources	Read			
PutResourcePolicy	Grants permission to attach a resource policy to an app monitor	Write	AppMonitorResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutRumEvents	Grants permission to put RUM events for appmonitor	Write	AppMonitorResource*		
PutRumMetricsDestination	Grants permission to put rum metrics destinations	Write	AppMonitorResource*		
TagResource	Grants permission to tag resources	Tagging	AppMonitorResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag resources	Tagging	AppMonitorResource*		
				aws:TagKeys	
UpdateAppMonitor	Grants permission to update appmonitor metadata	Write	AppMonitorResource*		iam:CreateServiceLinkedRole iam:GetRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRumMetricDefinition	Grants permission to update rum metric definition	Write	AppMonitorResource*		

Resource types defined by AWS CloudWatch RUM

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
AppMonitorResource	`arn:${Partition}:rum:${Region}:${Account}:appmonitor/${Name}`	aws:ResourceTag/${TagKey}

Condition keys for AWS CloudWatch RUM

AWS CloudWatch RUM defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed the request on behalf of the IAM principal	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource that make the request on behalf of the IAM principal	String
aws:TagKeys	Filters access by the tag keys that are passed in the request on behalf of the IAM principal	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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateResource	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} 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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
DeleteGroup	Grants permission to delete a group	Write	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Grants permission to list information of all canaries	Read		synthetics:Names	
DescribeCanariesLastRun	Grants permission to list information about the last test run associated with all canaries	Read		synthetics:Names	
DescribeRuntimeVersions	Grants permission to list information about Synthetics canary runtime versions	Read			
DisassociateResource	Grants permission to disassociate a resource from a group	Write	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCanary	Grants permission to view the details of a canary	Read	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Grants permission to list information about all the test runs associated with a canary	Read	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	Grants permission to view the details of a group	Read	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	Grants permission to list information about the associated groups of a canary	List	canary*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	Grants permission to list information about canaries in a group	List	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroups	Grants permission to list information of all groups	List			
ListTagsForResource	Grants permission to list all tags and values associated with a resource	Read	canary		
			group		
StartCanary	Grants permission to start a canary, so that Amazon CloudWatch Synthetics starts monitoring a website	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCanaryDryRun	Grants permission to start a canary dry run, so that Amazon CloudWatch Synthetics can execute a test execution of a canary with provided parameters	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	Grants permission to stop a canary	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to add one or more tags to a resource	Tagging	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	canary		
			group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Grants permission to update a canary	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Resource types defined by Amazon CloudWatch Synthetics

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
canary	`arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
group	arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString
synthetics:Names	Filters access based on the name of the canary	ArrayOfString

Actions, resources, and condition keys for AWS CodeArtifact

AWS CodeArtifact (service prefix: codeartifact) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS CodeArtifact

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateExternalConnection	Grants permission to add an external connection to a repository	Write	repository*		
AssociateWithDownstreamRepository	Grants permission to associate an existing repository as an upstream repository to another repository	Write	repository*		
CopyPackageVersions	Grants permission to copy package versions from one repository to another repository in the same domain	Write	package* repository*		
CreateDomain	Grants permission to create a new domain	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreatePackageGroup	Grants permission to create a package group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepository	Grants permission to create a new repository	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDomain	Grants permission to delete a domain	Write	domain*		
DeleteDomainPermissionsPolicy	Grants permission to delete the resource policy set on a domain	Permissions management	domain*		
DeletePackage	Grants permission to delete a package	Write	package*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePackageGroup	Grants permission to delete a package group	Write	package-group*		
DeletePackageVersions	Grants permission to delete package versions	Write	package*		
DeleteRepository	Grants permission to delete a repository	Write	repository*		
DeleteRepositoryPermissionsPolicy	Grants permission to delete the resource policy set on a repository	Permissions management	repository*		
DescribeDomain	Grants permission to return information about a domain	Read	domain*		
DescribePackage	Grants permission to retrieve information about a package	Read	package*		
DescribePackageGroup	Grants permission to return detailed information about a package group	Read	package-group*		
DescribePackageVersion	Grants permission to return information about a package version	Read	package*		
DescribeRepository	Grants permission to return detailed information about a repository	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateExternalConnection	Grants permission to disassociate an external connection from a repository	Write	repository*		
DisposePackageVersions	Grants permission to set the status of package versions to Disposed and delete their assets	Write	package*		
GetAssociatedPackageGroup	Grants permission to return a package's associated package group	Read	package-group*		
GetAuthorizationToken	Grants permission to generate a temporary authentication token for accessing repositories in a domain	Read	domain*		
GetDomainPermissionsPolicy	Grants permission to return a domain's resource policy	Read	domain*		
GetPackageVersionAsset	Grants permission to return an asset (or file) that is part of a package version	Read	package*		
GetPackageVersionReadme	Grants permission to return a package version's readme file	Read	package*		
GetRepositoryEndpoint	Grants permission to return an endpoint for a repository	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRepositoryPermissionsPolicy	Grants permission to return a repository's resource policy	Read	repository*		
ListAllowedRepositoriesForGroup	Grants permission to list the allowed repositories for a package group	List	package-group*		
ListAssociatedPackages	Grants permission to list the packages associated to a package group	List	package-group*		
ListDomains	Grants permission to list the domains in the current user's AWS account	List			
ListPackageGroups	Grants permission to list the package groups in a domain	List	domain*		
ListPackageVersionAssets	Grants permission to list a package version's assets	List	package*		
ListPackageVersionDependencies	Grants permission to list the direct dependencies of a package version	List	package*		
ListPackageVersions	Grants permission to list a package's versions	List	package*		
ListPackages	Grants permission to list the packages in a repository	List	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRepositories	Grants permission to list the repositories administered by the calling account	List			
ListRepositoriesInDomain	Grants permission to list the repositories in a domain	List	domain*		
ListSubPackageGroups	Grants permission to list the sub package groups for a parent package group	List	package-group*		
ListTagsForResource	Grants permission to list tags for a CodeArtifact resource	List	domain		
			package-group		
			repository		
PublishPackageVersion	Grants permission to publish assets and metadata to a repository endpoint	Write	package*		
PutDomainPermissionsPolicy	Grants permission to attach a resource policy to a domain	Write	domain*		
PutPackageMetadata	Grants permission to add, modify or remove package metadata using a repository endpoint	Write	package*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPackageOriginConfiguration	Grants permission to set origin configuration for a package	Write	package*		
PutRepositoryPermissionsPolicy	Grants permission to attach a resource policy to a repository	Write	repository*		
ReadFromRepository	Grants permission to return package assets and metadata from a repository endpoint	Read	repository*		
TagResource	Grants permission to tag a CodeArtifact resource	Tagging	domain		
			package-group		
			repository		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag from a CodeArtifact resource	Tagging	domain		
			package-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			repository		
				aws:TagKeys	
UpdatePackageGroup	Grants permission to modify the properties of a package group	Write	package-group*		
UpdatePackageGroupOriginConfiguration	Grants permission to modify the package origin configuration of a package group	Write	package-group*		
UpdatePackageVersionsStatus	Grants permission to modify the status of one or more versions of a package	Write	package*		
UpdateRepository	Grants permission to modify the properties of a repository	Write	repository*		

Resource types defined by AWS CodeArtifact

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 package groups resource must use an encoded package group pattern.

Resource types	ARN	Condition keys
domain	arn:${Partition}:codeartifact:${Region}:${Account}:domain/${DomainName}	aws:ResourceTag/${TagKey}
repository	arn:${Partition}:codeartifact:${Region}:${Account}:repository/${DomainName}/${RepositoryName}	aws:ResourceTag/${TagKey}
package-group	arn:${Partition}:codeartifact:${Region}:${Account}:package-group/${DomainName}${EncodedPackageGroupPattern}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:codeartifact:${Region}:${Account}:package/${DomainName}/${RepositoryName}/${PackageFormat}/${PackageNamespace}/${PackageName}	

Condition keys for AWS CodeArtifact

AWS CodeArtifact defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS CodeBuild

AWS 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 AWS CodeBuild
- Resource types defined by AWS CodeBuild
- Condition keys for AWS CodeBuild

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS CodeBuild build project that has its source code stored in a GitHub or Bitbucket repository, enables AWS 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 AWS 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 AWS CodeBuild build project that has its source code stored in a GitHub or Bitbucket repository, stops AWS 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 AWS 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 AWS CodeBuild console	List			
ListCuratedEnvironmentImages	Grants permission to get information about Docker images that are managed by AWS 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 AWS 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 AWS 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 AWS CodeBuild build project	Write	project*	codebuild:buildType codebuild:manualCreation codebuild:scopeConfiguration.domain codebuild:scopeConfiguration.name codebuild:scopeConfiguration.scope	

Resource types defined by AWS 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 AWS CodeBuild

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String
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 AWS 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 AWS 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 CodeCatalyst

Amazon CodeCatalyst (service prefix: `codecatalyst`) 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 CodeCatalyst

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptConnection [permission only]	Grants permission to accept a request to connect this account to an Amazon CodeCatalyst space	Write		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateIamRoleToConnection	Grants permission to associate an IAM role to a connection	Write	connections*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]				aws:ResourceTag/${TagKey}	
AssociateIdentityCenterApplicationToSpace [permission only]	Grants permission to associate an IAM Identity Center application with an Amazon CodeCatalyst space	Write	identity-center-application*		
				aws:ResourceTag/${TagKey}	
AssociateIdentityToIdentityCenterApplication [permission only]	Grants permission to associate an identity with an IAM Identity Center application for an Amazon CodeCatalyst space	Write	identity-center-application*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAssociateIdentitiesToIdentityCenterApplication [permission only]	Grants permission to associate multiple identities with an IAM Identity Center application for an Amazon CodeCatalyst space	Write	identity-center-application*		
				aws:ResourceTag/${TagKey}	
BatchDisassociateIdentitiesFromIdentityCenterApplication [permission only]	Grants permission to disassociate multiple identities from an IAM Identity Center application for an Amazon CodeCatalyst space	Write	identity-center-application*		
				aws:ResourceTag/${TagKey}	
CreateIdentityCenterApplication [permission only]	Grants permission to create an IAM Identity Center application	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSpace [permission only]	Grants permission to create an Amazon CodeCatalyst space	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSpaceAdminRoleAssignment [permission only]	Grants permission to create an administrator role assignment for a given Amazon CodeCatalyst space and IAM Identity Center application	Write	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DeleteConnection [permission only]	Grants permission to delete a connection	Write	connections*		
				aws:ResourceTag/${TagKey}	
DeleteIdentityCenterApplication [permission only]	Grants permission to delete an IAM Identity Center application	Write	identity-center-applications*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DisassociateIamRoleFromConnection [permission only]	Grants permission to disassociate an IAM role from a connection	Write	connections*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityCenterApplicationFromSpace [permission only]	Grants permission to disassociate an IAM Identity Center application from an Amazon CodeCatalyst space	Write	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
DisassociateIdentityFromIdentityCenterApplication [permission only]	Grants permission to disassociate an identity from an IAM Identity Center application for an Amazon CodeCatalyst space	Write	identity-center-applications*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetBillingAuthorization [permission only]	Grants permission to describe the billing authorization for a connection	Read	connections*		
				aws:ResourceTag/${TagKey}	
GetConnection [permission only]	Grants permission to get a connection	Read	connections*		
				aws:ResourceTag/${TagKey}	
GetIdentityCenterApplication [permission only]	Grants permission to get information about an IAM Identity Center application	Read	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPendingConnection [permission only]	Grants permission to get a pending request to connect this account to an Amazon CodeCatalyst space	Read			
ListConnections [permission only]	Grants permission to list connections that are not pending	List			
ListIamRolesForConnection [permission only]	Grants permission to list IAM roles associated with a connection	List	connections*		
				aws:ResourceTag/${TagKey}	
ListIdentityCenterApplications [permission only]	Grants permission to view a list of all IAM Identity Center applications in the account	List			
ListIdentityCenterApplicationsForSpace [permission only]	Grants permission to view a list of IAM Identity Center applications by Amazon CodeCatalyst space	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSpacesForIdentityCenterApplication [permission only]	Grants permission to view a list of Amazon CodeCatalyst spaces by IAM Identity Center application	List	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource [permission only]	Grants permission to list tags for an Amazon CodeCatalyst resource	Read	connections		
			identity-center-applications		
				aws:ResourceTag/${TagKey}	
PutBillingAuthorization [permission only]	Grants permission to create or update the billing authorization for a connection	Write	connections*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectConnection [permission only]	Grants permission to reject a request to connect this account to an Amazon CodeCatalyst space	Write			
SynchronizeIdentityCenterApplication [permission only]	Grants permission to synchronize an IAM Identity Center application with the backing identity store	Write	identity-center-applications*		
				aws:ResourceTag/${TagKey}	
TagResource [permission only]	Grants permission to tag an Amazon CodeCatalyst resource	Tagging	connections		
			identity-center-applications		

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 untag an Amazon CodeCatalyst resource	Tagging	connections		
			identity-center-applications		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIdentityCenterApplication [permission only]	Grants permission to update an IAM Identity Center application	Write	identity-center-applications*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon CodeCatalyst

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
connections	`arn:${Partition}:codecatalyst:${Region}:${Account}:/connections/${ConnectionId}`	aws:ResourceTag/${TagKey}
identity-center-applications	`arn:${Partition}:codecatalyst:${Region}:${Account}:/identity-center-applications/${IdentityCenterApplicationId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
space	arn:${Partition}:codecatalyst:::space/${SpaceId}	
project	arn:${Partition}:codecatalyst:::space/${SpaceId}/project/${ProjectId}	

Condition keys for Amazon CodeCatalyst

Amazon CodeCatalyst defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag's key and value in a request	String
aws:ResourceTag/${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

Actions, resources, and condition keys for AWS CodeCommit

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 attempting to merge two	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	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 AWS CodeCommit repository	Read	repository*		
BatchGetPullRequests [permission only]	Grants permission to return information about one or more pull requests in an AWS 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 AWS 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 AWS 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 AWS 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 AWS 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 AWS 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 AWS 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 AWS CodeCommit repository from the AWS CodeCommit console	Read	repository*		
GetBranch	Grants permission to get details about a branch in an AWS 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 AWS CodeCommit repository; does not control Git reference actions	Read	repository*		
GetRepository	Grants permission to get information about an AWS 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 AWS CodeCommit repository from the AWS 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 AWS CodePipeline	Read	repository*		
GitPull [permission only]	Grants permission to pull information from an AWS CodeCommit repository to a local repo	Read	repository*		
GitPush [permission only]	Grants permission to push information from a local repo to an AWS CodeCommit repository	Write	repository*		
				codecommit:References	
ListApprovalRuleTemplates	Grants permission to list all approval rule templates in an AWS Region for the AWS account	List			
ListAssociatedApprovalRuleTemplatesForRepository	Grants permission to list approval rule templates that are associated with a repository	List	repository*		
ListBranches	Grants permission to list branches for an AWS CodeCommit repository with this API; does not control Git branch actions	List	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS CodeCommit repositories in the current Region for your AWS 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		
MergeBranchesByFastForward	Grants permission to merge two commits into the specified destination branch using the fast-forward merge option	Write	repository*		
				codecommit:References	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFile	Grants permission to add or update a file in a branch in an AWS 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		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to disassociate resource tags from a CodeCommit resource ARN	Tagging	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDefaultBranch	Grants permission to change the default branch in an AWS CodeCommit repository	Write	repository*		
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 AWS CodeCommit repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRepositoryEncryptionKey	Grants permission to change the AWS KMS encryption key used to encrypt and decrypt an AWS CodeCommit repository	Write	repository*		
UpdateRepositoryName	Grants permission to change the name of an AWS CodeCommit repository	Write	repository*		
UploadArchive [permission only]	Grants permission to the service role for AWS CodePipeline to upload repository changes into a pipeline	Write	repository*		

Resource types defined by AWS 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 AWS CodeCommit

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
codecommit:References	Filters access by Git reference to specified AWS CodeCommit actions	String

Actions, resources, and condition keys for AWS CodeConnections

AWS CodeConnections (service prefix: `codeconnections`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CodeConnections

- Resource types defined by AWS CodeConnections
- Condition keys for AWS CodeConnections

Actions defined by AWS CodeConnections

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnection	Grants permission to create a Connection resource	Write		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:ProviderType	
CreateHost	Grants permission to create a host resource	Write		aws:RequestTag/${TagKey} aws:TagKeys codeconnections:Pr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				oviderType codeconnections:VpcId	
CreateRepositoryLink	Grants permission to create a repository link	Write	Connection*		codeconnections:PassConnection codeconnections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncConfiguration	Grants permission to create a template sync config	Write	RepositoryLink*		codeconnections:PassRepository iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codeconnections:Branch	
DeleteConnection	Grants permission to delete a Connection resource	Write	Connection*		
DeleteHost	Grants permission to delete a host resource	Write	Host*		
DeleteRepositoryLink	Grants permission to delete a repository link	Write	RepositoryLink*		
DeleteSyncConfiguration	Grants permission to delete a sync configuration	Write			
GetConnection	Grants permission to get details about a Connection resource	Read	Connection*		
GetConnectionToken [permission only]	Grants permission to get a Connection token to call provider actions	Read	Connection*		
GetHost	Grants permission to get details about a host resource	Read	Host*		
GetIndividualAccessToken [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codeconnections:ProviderType	codeconnections:StartOAuthHandshake

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstallationUrl [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codeconnections:ProviderType	
GetRepositoryLink	Grants permission to describe a repository link	Read	RepositoryLink*		
GetRepositorySyncStatus	Grants permission to get the latest sync status for a repository	Read	RepositoryLink*		
				codeconnections:Branch	
GetResourceSyncStatus	Grants permission to get the latest sync status for a resource (cfn stack or other resources)	Read			
GetSyncBlockerSummary	Grants permission to describe service sync blockers on a resource (cfn stack or other resources)	Read			
GetSyncConfiguration	Grants permission to describe a sync configuration	Read			
ListConnections	Grants permission to list Connection resources	List	Connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codeconnections:ProviderTypeFilter	
ListHosts	Grants permission to list host resources	List		codeconnections:ProviderTypeFilter	
ListInstallationTargets [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	List			codeconnections:GetIndividualAccessToken codeconnections:StartOAuthHandshake
ListRepositoryLinks	Grants permission to list repository links	List			
ListRepositorySyncDefinitions	Grants permission to list repository sync definitions	List			
ListSyncConfigurations	Grants permission to list sync configurations for a repository link	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to the set of key-value pairs that are used to manage the resource	List	Connection		
			Host		
			RepositoryLink		
PassConnection [permission only]	Grants permission to pass a Connection resource to an AWS service that accepts a Connection ARN as input, such as codepipeline:CreatePipeline	Read	Connection*		
				codeconnections:PassedToService	
PassRepository [permission only]	Grants permission to pass a repository link resource to an AWS service that accepts a RepositoryLinkId as input, such as codeconnections:CreateSyncConfiguration	Read	RepositoryLink*		
				codeconnections:PassedToService	
RegisterAppCode [permission only]	Grants permission to associate a third party server, such as a GitHub Enterprise Server instance, with a Host	Read		codeconnections:HostArn	
StartAppRegistrationHandshake [permission only]	Grants permission to associate a third party server, such as a GitHub Enterprise Server instance, with a Host	Read		codeconnections:HostArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartOAuthHandshake [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codeconnections:ProviderType	
TagResource	Grants permission to add or modify the tags of the given resource	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from an AWS resource	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnectionInstallation	Grants permission to update a Connection resource with an installation of the CodeStar Connections App	Write	Connection*		codeconnections:GetIndividualAccessToken codeconnections:GetInstallationUrl codeconnections:ListInstallationTargets codeconnections:StartOAuthHandshake
				codeconnections:InstallationId	
UpdateHost	Grants permission to update a host resource	Write	Host*		
				codeconnections:VpcId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRepositoryLink	Grants permission to update a repository link	Write	RepositoryLink*		
UpdateSyncBlocker	Grants permission to update a sync blocker for a resource (cfn stack or other resources)	Write			
UpdateSyncConfiguration	Grants permission to update a sync configuration	Write		codeconnections:Branch	
UseConnection [permission only]	Grants permission to use a Connection resource to call provider actions	Read	Connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codeconnections:BranchName codeconnections:FullRepositoryId codeconnections:OwnerId codeconnections:ProviderAction codeconnections:ProviderPermissionsRequired codeconnections:RepositoryName	

Resource types defined by AWS CodeConnections

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:${Partition}:codeconnections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codeconnections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codeconnections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS CodeConnections

AWS CodeConnections defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
codeconnections:Branch	Filters access by the branch name that is passed in the request	String
codeconnections:BranchName	Filters access by the branch name that is passed in the request. Applies only to UseConnection requests for access to a specific repository branch	String
codeconnections:FullRepositoryId	Filters access by the repository that is passed in the request. Applies only to UseConnection requests for access to a specific repository	String
codeconnections:HostArn	Filters access by the host resource associated with the connection used in the request	ARN
codeconnections:InstallationId	Filters access by the third-party ID (such as the Bitbucket App installation ID for CodeConnections) that is used to update a Connection. Allows you to restrict which third-party App installations can be used to make a Connection	String
codeconnections:OwnerId	Filters access by the owner of the third-party repository. Applies only to UseConnection requests for access to repositories owned by a specific user	String
codeconnections:PassedToService	Filters access by the service to which the principal is allowed to pass a Connection or RepositoryLink	String
codeconnections:ProviderAction	Filters access by the provider action in a UseConnection request such as ListRepositories. See documentation for all valid values	String

Condition keys	Description	Type
codeconnections:ProviderPermissionsRequired	Filters access by the write permissions of a provider action in a UseConnection request. Valid types include read_only and read_write	String
codeconnections:ProviderType	Filters access by the type of third-party provider passed in the request	String
codeconnections:ProviderTypeFilter	Filters access by the type of third-party provider used to filter results	String
codeconnections:RepositoryName	Filters access by the repository name that is passed in the request. Applies only to UseConnection requests for access to repositories owned by a specific user	String
codeconnections:VpcId	Filters access by the VpcId passed in the request	String

Actions, resources, and condition keys for AWS CodeDeploy

AWS 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 AWS CodeDeploy
- Resource types defined by AWS CodeDeploy

- Condition keys for AWS CodeDeploy

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [permission only]	Grants permission to create CloudFormation deployment to cooperate ochestration for a CloudFormation stack update	Write			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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 AWS 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/${TagKey}
deploymentconfig	`arn:${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 AWS CodeDeploy

AWS 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 AWS 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 AWS CodeDeploy secure host commands service

AWS 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 AWS CodeDeploy secure host commands service
- Resource types defined by AWS CodeDeploy secure host commands service
- Condition keys for AWS CodeDeploy secure host commands service

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
PutHostCommandComplete	Grants permission to mark host agent commands completed	Write			

Resource types defined by AWS CodeDeploy secure host commands service

AWS 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 AWS CodeDeploy secure host commands service, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for Amazon CodeGuru

Amazon CodeGuru (service prefix: `codeguru`) 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 CodeGuru

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCodeGuruFreeTrialSummary [permission only]	Grants permission to get free trial summary for the CodeGuru service which includes expiration date	Read			

Resource types defined by Amazon CodeGuru

Amazon CodeGuru does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon CodeGuru, specify `"Resource": "*"` in your policy.

Condition keys for Amazon CodeGuru

CodeGuru has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon CodeGuru Profiler

Amazon CodeGuru Profiler (service prefix: `codeguru-profiler`) 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 CodeGuru Profiler
- Resource types defined by Amazon CodeGuru Profiler
- Condition keys for Amazon CodeGuru Profiler

Actions defined by Amazon CodeGuru Profiler

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddNotificationChannels	Grants permission to add up to 2 topic ARNs of existing AWS SNS topics to publish notifications	Write	Profiling Group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetFrameMetricData	Grants permission to get the frame metric data for a Profiling Group	List	Profiling Group*		
ConfigureAgent	Grants permission to register with the orchestration service and retrieve profiling configuration information, used by agents	Write	Profiling Group*		
CreateProfilingGroup	Grants permission to create a profiling group	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteProfilingGroup	Grants permission to delete a profiling group	Write	Profiling Group*		
DescribeProfilingGroup	Grants permission to describe a profiling group	Read	Profiling Group*		
GetFindingsReportAccountSummary	Grants permission to get a summary of recent recommendations for each profiling group in the account	Read			
GetNotificationConfiguration	Grants permission to get the notification configuration	Read	Profiling Group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPolicy	Grants permission to get the resource policy associated with the specified Profiling Group	Read	Profiling Group*		
GetProfile	Grants permission to get aggregated profiles for a specific profiling group	Read	Profiling Group*		
GetRecommendations	Grants permission to get recommendations	Read	Profiling Group*		
ListFindingsReports	Grants permission to list the available recommendations reports for a specific profiling group	List	Profiling Group*		
ListProfileTimes	Grants permission to list the start times of the available aggregated profiles for a specific profiling group	List	Profiling Group*		
ListProfilingGroups	Grants permission to list profiling groups in the account	List			
ListTagsForResource	Grants permission to list tags for a Profiling Group	List	Profiling Group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PostAgentProfile	Grants permission to submit a profile collected by an agent belonging to a specific profiling group for aggregation	Write	Profiling Group*		
PutPermission	Grants permission to update the list of principals allowed for an action group in the resource policy associated with the specified Profiling Group	Permissions management	Profiling Group*		
RemoveNotificationChannel	Grants permission to delete an already configured SNStopic arn from the notification configuration	Write	Profiling Group*		
RemovePermission	Grants permission to remove the permission of specified Action Group from the resource policy associated with the specified Profiling Group	Permissions management	Profiling Group*		
SubmitFeedback	Grants permission to submit user feedback for useful or non useful anomaly	Write	Profiling Group*		
TagResource	Grants permission to add or overwrite tags to a Profiling Group	Tagging	Profiling Group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a Profiling Group	Tagging	Profiling Group*		
				aws:TagKeys	
UpdateProfilingGroup	Grants permission to update a specific profiling group	Write	Profiling Group*		

Resource types defined by Amazon CodeGuru Profiler

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
Profiling Group	`arn:${Partition}:codeguru-profiler:${Region}:${Account}:profilingGroup/${ProfilingGroupName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CodeGuru Profiler

Amazon CodeGuru Profiler defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer (service prefix: `codeguru-reviewer`) 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 CodeGuru Reviewer
- Resource types defined by Amazon CodeGuru Reviewer
- Condition keys for Amazon CodeGuru Reviewer

Actions defined by Amazon CodeGuru Reviewer

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Repository	Grants permission to associates a repository with Amazon CodeGuru Reviewer	Write		aws:RequestTag/${TagKey} aws:TagKeys	codecommit:GetRepository codecommit:ListRepositories codecommit:TagResource codestar-connections:PassConnection events:PutRule events:PutTargets iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:CreateBucket s3:ListBucket s3:PutBucketPolicy s3:PutLifecycleConfiguration
CreateCodeReview	Grants permission to create a code review	Write	association*		s3:GetObject
				aws:ResourceTag/${TagKey}	
CreateConnectionToken [permission only]	Grants permission to perform webbased oauth handshake for 3rd party providers	Read			
DescribeCodeReview	Grants permission to describe a code review	Read	association*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRecommendationFeedback	Grants permission to describe a recommendation feedback on a code review	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeRepositoryAssociation	Grants permission to describe a repository association	Read	association*		
				aws:ResourceTag/${TagKey}	
DisassociateRepository	Grants permission to disassociate a repository with Amazon CodeGuru Reviewer	Write	association*		codecommit:UntagResource events:DeleteRule events:RemoveTargets
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMetricsData [permission only]	Grants permission to view pull request metrics in console	Read			
ListCodeReviews	Grants permission to list summary of code reviews	List			
ListRecommendationFeedback	Grants permission to list summary of recommendation feedback on a code review	List	association*		
				aws:ResourceTag/${TagKey}	
ListRecommendations	Grants permission to list summary of recommendations on a code review	List	association*		
				aws:ResourceTag/${TagKey}	
ListRepositoryAssociations	Grants permission to list summary of repository associations	List			
ListTagsForResource	Grants permission to list the resource attached to a associated repository ARN	List	association*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListThirdPartyRepositories [permission only]	Grants permission to list 3rd party providers repositories in console	Read			
PutRecommendationFeedback	Grants permission to put feedback for a recommendation on a code review	Write	association*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to attach resource tags to an associated repository ARN	Tagging	association*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagResource	Grants permission to disassociate resource tags from an associated repository ARN	Tagging	association*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	

Resource types defined by Amazon CodeGuru Reviewer

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
association	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}`	aws:ResourceTag/${TagKey}
codereview	`arn:${Partition}:codeguru-reviewer:${Region}:${Account}:association:${ResourceId}:codereview:${CodeReviewId}`	

Condition keys for Amazon CodeGuru Reviewer

Amazon CodeGuru Reviewer defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CodeGuru Security

Amazon CodeGuru Security (service prefix: `codeguru-security`) 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 CodeGuru Security
- Resource types defined by Amazon CodeGuru Security
- Condition keys for Amazon CodeGuru Security

Actions defined by Amazon CodeGuru Security

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetFindings	Grants permission to batch retrieve specific findings generated by CodeGuru Security	Read	ScanName*		
CreateScan	Grants permission to create a CodeGuru Security scan	Write	ScanName*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUploadUrl	Grants permission to generate a presigned url for uploading code archives	Write	ScanName*		
DeleteScansByCategory [permission only]	Grants permission to delete all the scans and related findings from CodeGuru Security by given category	Write			
GetAccountConfiguration	Grants permission to retrieve the account level configurations	Read			
GetFindings	Grants permission to retrieve findings for a scan generated by CodeGuru Security	List	ScanName*		
GetMetricsSummary	Grants permission to retrieve AWS accout level metrics	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	summary generated by CodeGuru Security				
GetScan	Grants permission to retrieve CodeGuru Security scan metadata	Read	ScanName*		
				aws:ResourceTag/${TagKey}	
ListFindings [permission only]	Grants permission to retrieve findings generated by CodeGuru Security	List			
ListFindingsMetrics	Grants permission to retrieve a list of account level findings metrics within a date range	List			
ListScans	Grants permission to retrieve list of CodeGuru Security scan metadata	List			
ListTagsForResource	Grants permission to retrieve a list of tags for a scan name ARN	Read	ScanName*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to add tags to a scan name ARN	Tagging	ScanName*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a scan name ARN	Tagging	ScanName*		
				aws:TagKeys	
UpdateAccountConfiguration	Grants permission to update the account level configurations	Write			

Resource types defined by Amazon CodeGuru Security

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
ScanName	`arn:${Partition}:codeguru-security:${Region}:${Account}:scans/${ScanName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CodeGuru Security

Amazon CodeGuru Security defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS CodePipeline

AWS 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 AWS CodePipeline
- Resource types defined by AWS CodePipeline
- Condition keys for AWS CodePipeline

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account	Write	actiontype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Grants permission to create a uniquely named pipeline	Write	pipeline*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPipeline	Grants permission to retrieve information about a pipeline structure	Read	pipeline*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeployActionExecutionTargets	Grants permission to list the deployment details for deploy action executions that have occurred in a pipeline	Read	pipeline*		
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 AWS 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 AWS account	List	webhook*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
OverrideStageCondition	Grants permission to resume the pipeline execution by overriding a condition in a stage	Write	stage*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutJobSuccessResult	Grants permission to represent the success of a job as returned to the pipeline by a job worker (custom actions only)	Write			
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag from a CodePipeline resource	Tagging	actiontype		
			pipeline		
			webhook		
				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 AWS 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}
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 AWS CodePipeline

AWS 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 AWS 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

Condition keys	Description	Type
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 AWS CodeStar

AWS CodeStar (service prefix: `codestar`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CodeStar
- Resource types defined by AWS CodeStar
- Condition keys for AWS CodeStar

Actions defined by AWS CodeStar

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTeamMember	Grants permission to add a user to the team for an AWS CodeStar project	Permissions management	project*		
CreateProject	Grants permission to create a project with minimal structure, customer policies, and no resources	Permissions management		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Grants permission to create a profile for a user that includes user preferences, display name, and email	Write	user*		
DeleteExtendedAccess [permission only]	Grants permission to extended delete APIs	Write	project*		
DeleteProject	Grants permission to delete a project, including project resources. Does not delete users associated with the project, but does delete the IAM roles that allowed access to the project	Permissions management	project*		
DeleteUserProfile	Grants permission to delete a user profile in AWS CodeStar,	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	including all personal preference data associated with that profile, such as display name and email address. It does not delete the history of that user, for example the history of commits made by that user				
DescribeProject	Grants permission to describe a project and its resources	Read	project*		
DescribeUserProfile	Grants permission to describe a user in AWS CodeStar and the user attributes across all projects	Read			
DisassociateTeamMember	Grants permission to remove a user from a project. Removing a user from a project also removes the IAM policies from that user that allowed access to the project and its resources	Permissions management	project*		
GetExtendedAccess [permission only]	Grants permission to extended read APIs	Read	project*		
ListProjects	Grants permission to list all projects in CodeStar associated with your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResources	Grants permission to list all resources associated with a project in CodeStar	List	project*		
ListTagsForProject	Grants permission to list the tags associated with a project in CodeStar	List	project*		
ListTeamMembers	Grants permission to list all team members associated with a project	List	project*		
ListUserProfiles	Grants permission to list user profiles in AWS CodeStar	List			
PutExtendedAccess [permission only]	Grants permission to extended write APIs	Write	project*		
TagProject	Grants permission to add tags to a project in CodeStar	Tagging	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagProject	Grants permission to remove tags from a project in CodeStar	Tagging	project*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProject	Grants permission to update a project in CodeStar	Write	project*		
UpdateTeamMember	Grants permission to update team member attributes within a CodeStar project	Permissions management	project*		
UpdateUserProfile	Grants permission to update a profile for a user that includes user preferences, display name, and email	Write	user*		
VerifyServiceRole	Grants permission to verify whether the AWS CodeStar service role exists in the customer's account	List			

Resource types defined by AWS CodeStar

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:${Partition}:codestar:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
user	arn:${Partition}:iam::${Account}:user/${AwsUserName}	iam:ResourceTag/${TagKey}

Condition keys for AWS CodeStar

AWS CodeStar defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by requests based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag-value associated with the resource	String
aws:TagKeys	Filters access by requests based on the presence of mandatory tags in the request	ArrayOfString
iam:ResourceTag/${TagKey}	Filters access by actions based on tag-value associated with the resource	String

Actions, resources, and condition keys for AWS CodeStar Connections

AWS CodeStar Connections (service prefix: codestar-connections) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS CodeStar Connections

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnection	Grants permission to create a Connection resource	Write		aws:RequestTag/${TagKey} aws:TagKeys codestar-connections:ProviderType	
CreateHost	Grants permission to create a host resource	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys codestar-connections:ProviderType codestar-connections:VpcId	
CreateRepositoryLink	Grants permission to create a repository link	Write	Connection*		codestar-connections:PassConnection codestar-connections:UseConnection
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSyncConfiguration	Grants permission to create a template sync config	Write	RepositoryLink*		codestar-connections:PassRepository iam:PassRole
				codestar-connections:Branch	
DeleteConnection	Grants permission to delete a Connection resource	Write	Connection*		
DeleteHost	Grants permission to delete a host resource	Write	Host*		
DeleteRepositoryLink	Grants permission to delete a repository link	Write	RepositoryLink*		
DeleteSyncConfiguration	Grants permission to delete a sync configuration	Write			
GetConnection	Grants permission to get details about a Connection resource	Read	Connection*		
GetConnectionToken [permission only]	Grants permission to get a Connection token to call provider actions	Read	Connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHost	Grants permission to get details about a host resource	Read	Host*		
GetIndividualAccessToken [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codestar-connections:ProviderType	codestar-connections:StartOAuthHandshake
GetInstallationUrl [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codestar-connections:ProviderType	
GetRepositoryLink	Grants permission to describe a repository link	Read	RepositoryLink*		
GetRepositorySyncStatus	Grants permission to get the latest sync status for a repository	Read	RepositoryLink*		
				codestar-connections:Branch	
GetResourceSyncStatus	Grants permission to get the latest sync status for a resource (cfn stack or other resources)	Read			
GetSyncBlockerSummary	Grants permission to describe service sync blockers on a resource (cfn stack or other resources)	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSyncConfiguration	Grants permission to describe a sync configuration	Read			
ListConnections	Grants permission to list Connection resources	List	Connection*		
				codestar-connections:ProviderTypeFilter	
ListHosts	Grants permission to list host resources	List		codestar-connections:ProviderTypeFilter	
ListInstallationTargets [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	List			codestar-connections:GetIndividualAccessToken codestar-connections:StartOAuthHandshake
ListRepositoryLinks	Grants permission to list repository links	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRepositorySyncDefinitions	Grants permission to list repository sync definitions	List			
ListSyncConfigurations	Grants permission to list sync configurations for a repository link	List			
ListTagsForResource	Grants permission to the set of key-value pairs that are used to manage the resource	List	Connection		
			Host		
			RepositoryLink		
PassConnection [permission only]	Grants permission to pass a Connection resource to an AWS service that accepts a Connection ARN as input, such as codepipeline:CreatePipeline	Read	Connection*		
				codestar-connections:PassedToService	
PassRepository [permission only]	Grants permission to pass a repository link resource to an AWS service that accepts a RepositoryLinkId as input, such as codestar-connections:CreateSyncConfiguration	Read	RepositoryLink*		
				codestar-connections:PassedToService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterAppCode [permission only]	Grants permission to associate a third party server, such as a GitHub Enterprise Server instance, with a Host	Read		codestar-connections:HostArn	
StartAppRegistrationHandshake [permission only]	Grants permission to associate a third party server, such as a GitHub Enterprise Server instance, with a Host	Read		codestar-connections:HostArn	
StartOAuthHandshake [permission only]	Grants permission to associate a third party, such as a Bitbucket App installation, with a Connection	Read		codestar-connections:ProviderType	
TagResource	Grants permission to add or modify the tags of the given resource	Tagging	Connection		
			Host		
			RepositoryLink		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from an AWS resource	Tagging	Connection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Host		
			RepositoryLink		
				aws:TagKeys	
UpdateConnectionInstallation	Grants permission to update a Connection resource with an installation of the CodeStar Connections App	Write	Connection*		codestar-connections:GetIndividualAccessToken codestar-connections:GetInstallationUrl codestar-connections:ListInstallationTargets codestar-connections:StartOAuthHandshake

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codestar-connections:InstallationId	
UpdateHost	Grants permission to update a host resource	Write	Host*		
				codestar-connections:VpcId	
UpdateRepositoryLink	Grants permission to update a repository link	Write	RepositoryLink*		
UpdateSyncBlocker	Grants permission to update a sync blocker for a resource (cfn stack or other resources)	Write			
UpdateSyncConfiguration	Grants permission to update a sync configuration	Write		codestar-connections:Branch	
UseConnection [permission only]	Grants permission to use a Connection resource to call provider actions	Read	Connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codestar-connections:BranchName codestar-connections:FullRepositoryId codestar-connections:OwnerId codestar-connections:ProviderAction codestar-connections:ProviderPermissionsRequired codestar-connections:RepositoryName	

Resource types defined by AWS CodeStar Connections

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:${Partition}:codestar-connections:${Region}:${Account}:connection/${ConnectionId}`	aws:ResourceTag/${TagKey}
Host	`arn:${Partition}:codestar-connections:${Region}:${Account}:host/${HostId}`	aws:ResourceTag/${TagKey}
RepositoryLink	`arn:${Partition}:codestar-connections:${Region}:${Account}:repository-link/${RepositoryLinkId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS CodeStar Connections

AWS CodeStar Connections defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
codestar-connections:Branch	Filters access by the branch name that is passed in the request	String
codestar-connections:BranchName	Filters access by the branch name that is passed in the request. Applies only to UseConnection requests for access to a specific repository branch	String
codestar-connections:FullRepositoryId	Filters access by the repository that is passed in the request. Applies only to UseConnection requests for access to a specific repository	String
codestar-connections:HostArn	Filters access by the host resource associated with the connection used in the request	ARN
codestar-connections:InstallationId	Filters access by the third-party ID (such as the Bitbucket App installation ID for CodeStar Connections) that is used to update a Connection. Allows you to restrict which third-party App installations can be used to make a Connection	String
codestar-connections:OwnerId	Filters access by the owner of the third-party repository. Applies only to UseConnection requests for access to repositories owned by a specific user	String

Condition keys	Description	Type
codestar-connections:PassedToService	Filters access by the service to which the principal is allowed to pass a Connection or RepositoryLink	String
codestar-connections:ProviderAction	Filters access by the provider action in a UseConnection request such as ListRepositories. See documentation for all valid values	String
codestar-connections:ProviderPermissionsRequired	Filters access by the write permissions of a provider action in a UseConnection request. Valid types include read_only and read_write	String
codestar-connections:ProviderType	Filters access by the type of third-party provider passed in the request	String
codestar-connections:ProviderTypeFilter	Filters access by the type of third-party provider used to filter results	String
codestar-connections:RepositoryName	Filters access by the repository name that is passed in the request. Applies only to UseConnection requests for access to repositories owned by a specific user	String
codestar-connections:VpcId	Filters access by the VpcId passed in the request	String

Actions, resources, and condition keys for AWS CodeStar Notifications

AWS CodeStar Notifications (service prefix: `codestar-notifications`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS CodeStar Notifications

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNotificationRule	Grants permission to create a notification rule for a resource	Write	notificationrule*		
				aws:RequestTag/${TagKey} aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteNotificationRule	Grants permission to delete a notification rule for a resource	Write	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
DeleteTarget	Grants permission to delete a target for a notification rule	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DescribeNotificationRule	Grants permission to get information about a notification rule	Read	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
ListEventTypes	Grants permission to list notifications event types	List			
ListNotificationRules	Grants permission to list notification rules in an AWS account	List			
ListTagsForResource	Grants permission to list the tags attached to a notification rule resource ARN	List	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTargets	Grants permission to list the notification rule targets for an AWS account	List		aws:RequestTag/${TagKey} aws:TagKeys	
Subscribe	Grants permission to create an association between a notification rule and an Amazon SNS topic	Write	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
TagResource	Grants permission to attach resource tags to a notification rule resource ARN	Tagging	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	Grants permission to remove an association between a notification rule and an Amazon SNS topic	Write	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	
UntagResource	Grants permission to disassociate resource tags from a notification rule resource ARN	Tagging	notificationrule*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateNotificationRule	Grants permission to change a notification rule for a resource	Write	notificationrule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys codestar-notifications:NotificationsForResource	

Resource types defined by AWS CodeStar 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
notificationrule	`arn:${Partition}:codestar-notifications:${Region}:${Account}:notificationrule/${NotificationRuleId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS CodeStar Notifications

AWS CodeStar Notifications defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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
codestar-notifications:NotificationsForResource	Filters access based on the ARN of the resource for which notifications are configured	ARN

Actions, resources, and condition keys for Amazon CodeWhisperer

Amazon CodeWhisperer (service prefix: `codewhisperer`) 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 CodeWhisperer

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for CodeWhisperer customization resource	Permissions management	customization*		
				aws:ResourceTag/${TagKey}	
AssociateCustomizationPermi	Grants permission to invoke AssociateCustomizationPermission on CodeWhisperer	Write	customization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ssion [permission only]				aws:ResourceTag/${TagKey}	
CreateCustomization [permission only]	Grants permission to invoke CreateCustomization on CodeWhisperer	Write	customization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProfile [permission only]	Grants permission to invoke CreateProfile on CodeWhisperer	Write	profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCustomization [permission only]	Grants permission to invoke DeleteCustomization on CodeWhisperer	Write	customization*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProfile [permission only]	Grants permission to invoke DeleteProfile on CodeWhisperer	Write	profile*		
				aws:ResourceTag/${TagKey}	
DisassociateCustomizationPermission [permission only]	Grants permission to invoke DisassociateCustomizationPermission on CodeWhisperer	Write	customization*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations [permission only]	Grants permission to invoke GenerateRecommendations on CodeWhisperer	Read			
GetCustomization [permission only]	Grants permission to invoke GetCustomization on CodeWhisperer	Read	customization*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCustomizationPermissions [permission only]	Grants permission to invoke ListCustomizationPermissions on CodeWhisperer	List	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizationVersions [permission only]	Grants permission to invoke ListCustomizationVersions on CodeWhisperer	List	customization*		
				aws:ResourceTag/${TagKey}	
ListCustomizations [permission only]	Grants permission to invoke ListCustomizations on CodeWhisperer	List	customization*		
ListProfiles [permission only]	Grants permission to invoke ListProfiles on CodeWhisperer	List			
ListTagsForResource [permission only]	Grants permission to invoke ListTagsForResource on CodeWhisperer	List	customization		
			profile		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource [permission only]	Grants permission to invoke TagResource on CodeWhisperer	Tagging	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [permission only]	Grants permission to invoke UntagResource on CodeWhisperer	Tagging	customization		
			profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCustomization [permission only]	Grants permission to invoke UpdateCustomization on CodeWhisperer	Write	customization*		
				aws:ResourceTag/${TagKey}	
UpdateProfile [permission only]	Grants permission to invoke UpdateProfile on CodeWhisperer	Write	profile*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon CodeWhisperer

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:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
customization	arn:${Partition}:codewhisperer:${Region}:${Account}:customization/${Identifier}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CodeWhisperer

Amazon CodeWhisperer defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with CodeWhisperer resource	String
aws:TagKeys	Filters access by the tag keys that are passed 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		cognito-identity:IdentityPoolArn	
DeleteIdentityPool	Grants permission to delete a user pool. Once a pool is	Write	identitypool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	deleted, users will not be able to authenticate with the pool				
DescribeIdentity	Grants permission to return metadata related to the given identity, including when the identity was created and any associated linked logins	Read		cognito-identity:IdentityPoolArn	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCredentialsForIdentity	Grants permission to return credentials for the provided identity ID	Read		cognito-identity-unauth:IdentityPoolArn cognito-identity-unauth:AccountId cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetId	Grants permission to generate (or retrieve) a Cognito ID. Supplying multiple logins will create an implicit linked account	Write		cognito-identity-unauth:IdentityPoolArn cognito-identity-unauth:AccountId cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	
GetIdentityPoolAnalytics	Grants permission to get analytics data about the total current identity count for all identity pool identity provider (IdPs)	Read	identitypool*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		cognito-identity-unauth:IdentityPoolArn cognito-identity-unauth:AccountId cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnlinkIdentity	Grants permission to unlink a federated identity from an existing account	Write		cognito-identity-auth:IdentityPoolArn cognito-identity-auth:AccountId	
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 AWS 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 a key that is present in the request	ArrayOfString
cognito-identity-auth:AccountId	Filters access by the owning AWS account ID for identity pool authenticated users. Applies to unauthenticated (public) API operations	String
cognito-identity-auth:IdentityPoolArn	Filters access by the identity pool ID for a given authenticated-user identity ID. Applies to unauthenticated (public) API operations	ARN

Condition keys	Description	Type
cognito-identity-unauth:AccountId	Filters access by the owning AWS account ID of an identity pool for identity pool guest users. Applies to unauthenticated (public) API operations	String
cognito-identity-unauth:IdentityPoolArn	Filters access by the identity pool ID for a given guest-user identity ID. Applies to unauthenticated (public) API operations	ARN
cognito-identity:IdentityPoolArn	Filters access by the identity pool ID for a given identity ID for DeleteIdentities and DescribeIdentity	ARN

Actions, resources, and condition keys for Amazon Cognito Sync

Amazon Cognito Sync (service prefix: `cognito-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 Cognito Sync
- Resource types defined by Amazon Cognito Sync
- Condition keys for Amazon Cognito Sync

Actions defined by Amazon Cognito 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BulkPublish	Grants permission to initiate a bulk publish of all existing datasets for an Identity Pool to the configured stream	Write	identitypool*		
DeleteDataset	Grants permission to delete a specific dataset	Write	dataset*		
DescribeDataset	Grants permission to get metadata about a dataset by identity and dataset name	Read	dataset*		
DescribeIdentityPoolUsage	Grants permission to get usage details (for example, data storage) about a particular identity pool	Read	identitypool*		
DescribeIdentityUsage	Grants permission to get usage information for an identity, including number of datasets and data usage	Read	identity*		
GetBulkPublishDetails	Grants permission to get the status of the last BulkPublish operation for an identity pool	Read	identitypool*		
GetCognitoEvents	Grants permission to get the events and the corresponding Lambda functions associated with an identity pool	Read	identitypool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdentityPoolConfiguration	Grants permission to get the configuration settings of an identity pool	Read	identitypool*		
ListDatasets	Grants permission to list datasets for an identity	List	dataset*		
ListIdentityPoolUsage	Grants permission to get a list of identity pools registered with Cognito	Read	identitypool*		
ListRecords	Grants permission to get paginated records, optionally changed after a particular sync count for a dataset and identity	Read	dataset*		
QueryRecords [permission only]	Grants permission to query records	Read			
RegisterDevice	Grants permission to register a device to receive push sync notifications	Write	identity*		
SetCognitoEvents	Grants permission to set the AWS Lambda function for a given event type for an identity pool	Write	identitypool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetDatasetConfiguration [permission only]	Grants permission to configure datasets	Write	dataset*		
SetIdentityPoolConfiguration	Grants permission to set the necessary configuration for push sync	Write	identitypool*		
SubscribeToDataset	Grants permission to subscribe to receive notifications when a dataset is modified by another device	Write	dataset*		
UnsubscribeFromDataset	Grants permission to unsubscribe from receiving notifications when a dataset is modified by another device	Write	dataset*		
UpdateRecords	Grants permission to post updates to records and add and delete records for a dataset and user	Write	dataset*		

Resource types defined by Amazon Cognito 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
dataset	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}/dataset/${DatasetName}`	
identity	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}/identity/${IdentityId}`	
identitypool	`arn:${Partition}:cognito-sync:${Region}:${Account}:identitypool/${IdentityPoolId}`	

Condition keys for Amazon Cognito Sync

Cognito 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 AWS global condition context keys.

Actions, resources, and condition keys for Amazon Cognito User Pools

Amazon Cognito User Pools (service prefix: `cognito-idp`) 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 User Pools
- Resource types defined by Amazon Cognito User Pools

- Condition keys for Amazon Cognito User Pools

Actions defined by Amazon Cognito User Pools

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCustomAttributes	Grants permission to add user attributes to the user pool schema	Write	userpool*		
AddUserPoolClientSecret	Grants permission to add a new secret to a confidential client	Write	userpool*		
AdminAddUserToGroup	Grants permission to add any user to any group	Write	userpool*		
AdminConfirmSignUp	Grants permission to confirm any user's registration without a confirmation code	Write	userpool*		
AdminCreateUser	Grants permission to create new users and send welcome messages via email or SMS	Write	userpool*		
AdminDeleteUser	Grants permission to delete any user	Write	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AdminDeleteUserAttributes	Grants permission to delete attributes from any user	Write	userpool*		
AdminDisableProviderForUser	Grants permission to unlink any user pool user from a third-party identity provider (IdP) user	Write	userpool*		
AdminDisableUser	Grants permission to deactivate any user	Write	userpool*		
AdminEnableUser	Grants permission to activate any user	Write	userpool*		
AdminForgetDevice	Grants permission to deregister any user's devices	Write	userpool*		
AdminGetDevice	Grants permission to get information about any user's devices	Read	userpool*		
AdminGetUser	Grants permission to look up any user by user name	Read	userpool*		
AdminInitiateAuth	Grants permission to authenticate any user	Write	userpool*		
AdminLinkProviderForUser	Grants permission to link any user pool user to a third-party IdP user	Write	userpool*		
AdminListDevices	Grants permission to list any user's remembered devices	List	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AdminListGroupsForUser	Grants permission to list the groups that any user belongs to	List	userpool*		
AdminListUserAuthEvents	Grants permission to lists sign-in events for any user	Read	userpool*		
AdminRemoveUserFromGroup	Grants permission to remove any user from any group	Write	userpool*		
AdminResetUserPassword	Grants permission to reset any user's password	Write	userpool*		
AdminRespondToAuthChallenge	Grants permission to respond to an authentication challenge during the authentication of any user	Write	userpool*		
AdminSetUserMFAPreference	Grants permission to set any user's preferred MFA method	Write	userpool*		
AdminSetUserPassword	Grants permission to set any user's password	Write	userpool*		
AdminSetUserSettings	Grants permission to set user settings for any user	Write	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AdminUpdateAuthEventFeedback	Grants permission to update advanced security feedback for any user's authentication event	Write	userpool*		
AdminUpdateDeviceStatus	Grants permission to update the status of any user's remembered devices	Write	userpool*		
AdminUpdateUserAttributes	Grants permission to updates any user's standard or custom attributes	Write	userpool*		
AdminUserGlobalSignOut	Grants permission to sign out any user from all sessions	Write	userpool*		
AssociateSoftwareToken	Grants permission to return a unique generated shared secret key code for the user	Write			
AssociateWebACL [permission only]	Grants permission to associate the user pool with an AWS WAF web ACL	Write	userpool* webacl*		
ChangePassword	Grants permission to change the password for a specified user in a user pool	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfirmDevice	Grants permission to confirm tracking of the device. This API call is the call that begins device tracking	Write			
ConfirmForgotPassword	Grants permission to allow a user to enter a confirmation code to reset a forgotten password	Write			
ConfirmSignUp	Grants permission to confirm registration of a user and handles the existing alias from a previous user	Write			
CreateGroup	Grants permission to create new user pool groups	Write	userpool*		
CreateIdentityProvider	Grants permission to add identity providers to user pools	Write	userpool*		
CreateManagedLoginBranding	Grants permission to create a branding settings for managed login and associate it with an app client	Write	userpool*		
CreateResourceServer	Grants permission to create and configure scopes for OAuth 2.0 resource servers	Write	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTerms	Grants permission to create terms and associate it with an app client	Write	userpool*		
CreateUserImportJob	Grants permission to create user CSV import jobs	Write	userpool*		
CreateUserPool	Grants permission to create and set password policy for user pools	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateUserPoolClient	Grants permission to create user pool app clients	Write	userpool*		
CreateUserPoolDomain	Grants permission to add user pool domains	Write	userpool*		
DeleteGroup	Grants permission to delete any empty user pool group	Write	userpool*		
DeleteIdentityProvider	Grants permission to delete any identity provider from user pools	Write	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteManagedLoginBranding	Grants permission to delete the managed login branding style for any app client	Write	userpool*		
DeleteResourceServer	Grants permission to delete any OAuth 2.0 resource server from user pools	Write	userpool*		
DeleteTerms	Grants permission to delete terms for an app client	Write	userpool*		
DeleteUser	Grants permission to allow a user to delete one's self	Write			
DeleteUserAttributes	Grants permission to delete the attributes for a user	Write			
DeleteUserPool	Grants permission to delete user pools	Write	userpool*		
DeleteUserPoolClient	Grants permission to delete any user pool app client	Write	userpool*		
DeleteUserPoolClientSecret	Grants permission to delete a secret from a list of secrets associated with a client	Write	userpool*		
DeleteUserPoolDomain	Grants permission to delete any user pool domain	Write	userpool*		
DescribeIdentityProvider	Grants permission to describe any user pool identity provider	Read	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeManagedLoginBranding	Grants permission to get the detailed information about the branding style of managed login	Read	userpool*		
DescribeManagedLoginBrandingByClient	Grants permission to get the detailed information about the branding style of managed login associated with an appclient	Read	userpool*		
DescribeResourceServer	Grants permission to describe any OAuth 2.0 resource server	Read	userpool*		
DescribeRiskConfiguration	Grants permission to describe the risk configuration settings of user pools and app clients	Read	userpool*		
DescribeTerms	Grants permission to get the detailed information about terms for an app client	Read	userpool*		
DescribeUserImportJob	Grants permission to describe any user import job	Read	userpool*		
DescribeUserPool	Grants permission to describe user pools	Read	userpool*		
DescribeUserPoolClient	Grants permission to describe any user pool app client	Read	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeUserPoolDomain	Grants permission to describe any user pool domain	Read			
DisassociateWebACL [permission only]	Grants permission to disassociate the user pool with an AWS WAF web ACL	Write	userpool*		
ForgetDevice	Grants permission to forget the specified device	Write			
ForgotPassword	Grants permission to send a message to the end user with a confirmation code that is required to change the user's password	Write			
GetCSVHeader	Grants permission to generate headers for a user import .csv file	Read	userpool*		
GetDevice	Grants permission to get the device	Read			
GetGroup	Grants permission to describe a user pool group	Read	userpool*		
GetIdentityProviderByIdentifier	Grants permission to correlate a user pool IdP identifier to the IdP Name	Read	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLogDeliveryConfiguration	Grants permission to get the detailed activity logging configuration for a user pool	Read	userpool*		
GetSigningCertificate	Grants permission to look up signing certificates for user pools	Read	userpool*		
GetTokensFromRefreshToken	Grants permission to update user tokens with refresh tokens	Write			
GetUICustomization	Grants permission to get UI customization information for the hosted UI of any app client	Read	userpool*		
GetUser	Grants permission to get the user attributes and metadata for a user	Read			
GetUserAttributeVerificationCode	Grants permission to get the user attribute verification code for the specified attribute name	Read			
GetUserPoolMfaConfig	Grants permission to look up the MFA configuration of user pools	Read	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWebACLForResource [permission only]	Grants permission to get the AWS WAF web ACL that is associated with an Amazon Cognito user pool	Read	userpool*		
GlobalSignOut	Grants permission to sign out users from all devices	Write			
InitiateAuth	Grants permission to initiate the authentication flow	Write			
ListDevices	Grants permission to list the devices	List			
ListGroups	Grants permission to list all groups in user pools	List	userpool*		
ListIdentityProviders	Grants permission to list all identity providers in user pools	List	userpool*		
ListResourceServers	Grants permission to list all resource servers in user pools	List	userpool*		
ListResourcesForWebACL [permission only]	Grants permission to list the user pools that are associated with an AWS WAF web ACL	List	webacl*		
ListTagsForResource	Grants permission to list the tags that are assigned to an Amazon Cognito user pool	List	userpool		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTerms	Grants permission to list all terms for a user pool	List	userpool*		
ListUserImportJobs	Grants permission to list all user import jobs	List	userpool*		
ListUserPoolClientSecrets	Grants permission to list all secrets associated with a client	List	userpool*		
ListUserPoolClients	Grants permission to list all app clients in user pools	List	userpool*		
ListUserPools	Grants permission to list all user pools	List			
ListUsers	Grants permission to list all user pool users	List	userpool*		
ListUsersInGroup	Grants permission to list the users in any group	List	userpool*		
ResendConfirmationCode	Grants permission to resend the confirmation (for confirmation of registration) to a specific user in the user pool	Write			
RespondToAuthChallenge	Grants permission to respond to the authentication challenge	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeToken	Grants permission to revoke all of the access tokens generated by the specified refresh token	Write			
SetLogDeliveryConfiguration	Grants permission to set up or modify the detailed activity logging configuration of a user pool	Write	userpool*		
SetRiskConfiguration	Grants permission to set risk configuration for user pools and app clients	Write	userpool*		
SetUICustomization	Grants permission to customize the hosted UI for any app client	Write	userpool*		
SetUserMFAPreference	Grants permission to set MFA preference for the user in the userpool	Write			
SetUserPoolMfaConfig	Grants permission to set user pool MFA configuration	Write	userpool*		
SetUserSettings	Grants permission to set the user settings like multi-factor authentication (MFA)	Write			
SignUp	Grants permission to register the user in the specified user pool and creates a user name, password, and user attributes	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartUserImportJob	Grants permission to start any user import job	Write	userpool*		
StopUserImportJob	Grants permission to stop any user import job	Write	userpool*		
TagResource	Grants permission to tag a user pool	Tagging	userpool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a user pool	Tagging	userpool		
				aws:TagKeys	
UpdateAuthEventFeedback	Grants permission to update the feedback for the user authentication event	Write	userpool*		
UpdateDeviceStatus	Grants permission to update the device status	Write			
UpdateGroup	Grants permission to update the configuration of any group	Write	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIdentityProvider	Grants permission to update the configuration of any user pool IdP	Write	userpool*		
UpdateManagedLoginBranding	Grants permission to update the branding settings of a managed login	Write	userpool*		
UpdateResourceServer	Grants permission to update the configuration of any OAuth 2.0 resource server	Write	userpool*		
UpdateTerms	Grants permission to update terms for an app client	Write	userpool*		
UpdateUserAttributes	Grants permission to allow a user to update a specific attribute (one at a time)	Write			
UpdateUserPool	Grants permission to updates the configuration of user pools	Write	userpool*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateUserPoolClient	Grants permission to update any user pool client	Write	userpool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUserPoolDomain	Grants permission to replace the certificate for any custom domain	Write	userpool*		
VerifySoftwareToken	Grants permission to register a user's entered TOTP code and mark the user's software token MFA status as verified if successful	Write			
VerifyUserAttribute	Grants permission to verify a user attribute using a one time verification code	Write			

Resource types defined by Amazon Cognito User Pools

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
userpool	`arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}`	aws:ResourceTag/${TagKey}
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	

Condition keys for Amazon Cognito User Pools

Amazon Cognito User Pools defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by a key that is present in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Comprehend

Amazon Comprehend (service prefix: `comprehend`) 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 Comprehend
- Resource types defined by Amazon Comprehend
- Condition keys for Amazon Comprehend

Actions defined by Amazon Comprehend

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDetectDominantLanguage	Grants permission to detect the language or languages present in the list of text documents	Read			
BatchDetectEntities	Grants permission to detect the named entities ("People", "Places", "Locations", etc) within the given list of text documents	Read			
BatchDetectKeyPhrases	Grants permission to detect the phrases in the list of text documents that are most indicative of the content	Read			
BatchDetectSentiment	Grants permission to detect the sentiment of a text in the list of documents (Positive, Negative, Neutral, or Mixed)	Read			
BatchDetectSyntax	Grants permission to detect syntactic information (like Part of Speech, Tokens) in a list of text documents	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDetectTargetedSentiment	Grants permission to detect the sentiments associated with specific entities (such as brands or products) within the given list of text documents	Read			
ClassifyDocument	Grants permission to create a new document classification request to analyze a single document in real-time, using a previously created and trained custom model and an endpoint	Read	document-classifier-endpoint*		
ContainsPiiEntities	Grants permission to classify the personally identifiable information within given documents in real-time	Read			
CreateDataset	Grants permission to create a new dataset within a flywheel	Write	flywheel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDocumentClassifier	Grants permission to create a new document classifier that you can use to categorize documents	Write	document-classifier*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEndpoint	Grants permission to create a model-specific endpoint for synchronous inference for a previously trained custom model	Write	document-classifier*		
			document-classifier-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			entity-recognizer*		
			entity-recognizer-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	
			flywheel		
CreateEntityRecognizer	Grants permission to create an entity recognizer using submitted files	Write	entity-recognizer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFlywheel	Grants permission to create a new flywheel that you can use to train model versions	Write	flywheel*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:DataLakeKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDocumentClassifier	Grants permission to delete a previously created document classifier	Write	document-classifier*		
DeleteEndpoint	Grants permission to delete a model-specific endpoint for a previously-trained custom model. All endpoints must be deleted in order for the model to be deleted	Write	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DeleteEntityRecognizer	Grants permission to delete a submitted entity recognizer	Write	entity-recognizer*		
DeleteFlywheel	Grants permission to Delete a flywheel	Write	flywheel*		
DeleteResourcePolicy	Grants permission to remove policy on resource	Write	document-classifier*		
			entity-recognizer*		
DescribeDataset	Grants permission to get the properties associated with a dataset	Read	flywheel-dataset*		
DescribeDocumentClassificationJob	Grants permission to get the properties associated with a document classification job	Read	document-classification-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDocumentClassifier	Grants permission to get the properties associated with a document classifier	Read	document-classifier*		
DescribeDominantLanguageDetectionJob	Grants permission to get the properties associated with a dominant language detection job	Read	dominant-language-detection-job*		
DescribeEndpoint	Grants permission to get the properties associated with a specific endpoint. Use this operation to get the status of an endpoint	Read	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
DescribeEntitiesDetectionJob	Grants permission to get the properties associated with an entities detection job	Read	entities-detection-job*		
DescribeEntityRecognizer	Grants permission to provide details about an entity recognizer including status, S3 buckets containing training data, recognizer metadata, metrics, and so on	Read	entity-recognizer*		
DescribeEventsDetectionJob	Grants permission to get the properties associated with an Events detection job	Read	events-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFlywheel	Grants permission to get the properties associated with a flywheel	Read	flywheel*		
DescribeFlywheelIteration	Grants permission to get the properties associated with a flywheel iteration for a flywheel	Read	flywheel*		
				comprehend:FlywheelIterationId	
DescribeKeyPhrasesDetectionJob	Grants permission to get the properties associated with a key phrases detection job	Read	key-phrases-detection-job*		
DescribePiiEntitiesDetectionJob	Grants permission to get the properties associated with a PII entities detection job	Read	pii-entities-detection-job*		
DescribeResourcePolicy	Grants permission to read attached policy on resource	Read	document-classifier*		
			entity-recognizer*		
DescribeSentimentDetectionJob	Grants permission to get the properties associated with a sentiment detection job	Read	sentiment-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTargetedSentimentDetectionJob	Grants permission to get the properties associated with a targeted sentiment detection job	Read	targeted-sentiment-detection-job*		
DescribeTopicsDetectionJob	Grants permission to get the properties associated with a topic detection job	Read	topics-detection-job*		
DetectDominantLanguage	Grants permission to detect the language or languages present in the text	Read			
DetectEntities	Grants permission to detect the named entities ("People", "Places", "Locations", etc) within the given text document	Read	entity-recognizer-endpoint		
DetectKeyPhrases	Grants permission to detect the phrases in the text that are most indicative of the content	Read			
DetectPiiEntities	Grants permission to detect the personally identifiable information entities ("Name", "SSN", "PIN", etc) within the given text document	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetectSentiment	Grants permission to detect the sentiment of a text in a document (Positive, Negative, Neutral, or Mixed)	Read			
DetectSyntax	Grants permission to detect syntactic information (like Part of Speech, Tokens) in a text document	Read			
DetectTargetedSentiment	Grants permission to detect the sentiments associated with specific entities (such as brands or products) in a document	Read			
DetectToxicContent	Grants permission to detect toxic content within the given list of text segments	Read			
ImportModel	Grants permission to import a trained Comprehend model	Write	document-classifier*		
			entity-recognizer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:ModelKmsKey	
ListDatasets	Grants permission to get a list of the Datasets associated with a flywheel	Read	flywheel*		
ListDocumentClassificationJobs	Grants permission to get a list of the document classification jobs that you have submitted	Read			
ListDocumentClassifierSummaries	Grants permission to get a list of summaries of the document classifiers that you have created	Read			
ListDocumentClassifiers	Grants permission to get a list of the document classifiers that you have created	Read			
ListDominantLanguageDetectionJobs	Grants permission to get a list of the dominant language detection jobs that you have submitted	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEndpoints	Grants permission to get a list of all existing endpoints that you've created	Read			
ListEntitiesDetectionJobs	Grants permission to get a list of the entity detection jobs that you have submitted	Read			
ListEntityRecognizerSummaries	Grants permission to get a list of summaries for the entity recognizers that you have created	Read			
ListEntityRecognizers	Grants permission to get a list of the properties of all entity recognizers that you created, including recognizers currently in training	Read			
ListEventsDetectionJobs	Grants permission to get a list of Events detection jobs that you have submitted	Read			
ListFlywheelIterationHistory	Grants permission to get a list of iterations associated for a flywheel	Read	flywheel*		
ListFlywheels	Grants permission to get a list of the flywheels that you have created	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListKeyPhrasesDetectionJobs	Grants permission to get a list of key phrase detection jobs that you have submitted	Read			
ListPiiEntitiesDetectionJobs	Grants permission to get a list of PII entities detection jobs that you have submitted	Read			
ListSentimentDetectionJobs	Grants permission to get a list of sentiment detection jobs that you have submitted	Read			
ListTagsForResource	Grants permission to list tags for a resource	Read	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			entity-recognizer-endpoint		
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			topics-detection-job		
ListTargetedSentimentDetectionJobs	Grants permission to get a list of targeted sentiment detection jobs that you have submitted	Read			
ListTopicsDetectionJobs	Grants permission to get a list of the topic detection jobs that you have submitted	Read			
PutResourcePolicy	Grants permission to attach policy to resource	Write	document-classifier*		
			entity-recognizer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDocumentClassificationJob	Grants permission to start an asynchronous document classification job	Write	document-classification-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			flywheel		
StartDominantLanguageDetectionJob	Grants permission to start an asynchronous dominant language detection job for a collection of documents	Write	dominant-language-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartEntitiesDetectionJob	Grants permission to start an asynchronous entity detection job for a collection of documents	Write	entities-detection-job*	aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			entity-recognizer		
			flywheel		
StartEventsDetectionJob	Grants permission to start an asynchronous Events detection job for a collection of documents	Write	events-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartFlywheelIteration	Grants permission to start a flywheel iteration for a flywheel	Write	flywheel*		
StartKeyPhrasesDetectionJob	Grants permission to start an asynchronous key phrase detection job for a collection of documents	Write	key-phrases-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartPiiEntitiesDetectionJob	Grants permission to start an asynchronous PII entities detection job for a collection of documents	Write	pii-entities-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:OutputKmsKey	
StartSentimentDetectionJob	Grants permission to start an asynchronous sentiment detection job for a collection of documents	Write	sentiment-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StartTargetedSentimentDetectionJob	Grants permission to start an asynchronous targeted sentiment detection job for a collection of documents	Write	targeted-sentiment-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTopicsDetectionJob	Grants permission to start an asynchronous job to detect the most common topics in the collection of documents and the phrases associated with each topic	Write	topics-detection-job*		
				aws:RequestTag/${TagKey} aws:TagKeys comprehend:VolumeKmsKey comprehend:OutputKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
StopDominantLanguageDetectionJob	Grants permission to stop a dominant language detection job	Write	dominant-language-detection-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEntitiesDetectionJob	Grants permission to stop an entity detection job	Write	entities-detection-job*		
StopEventsDetectionJob	Grants permission to stop an Events detection job	Write	events-detection-job*		
StopKeyPhrasesDetectionJob	Grants permission to stop a key phrase detection job	Write	key-phrases-detection-job*		
StopPiiEntitiesDetectionJob	Grants permission to stop a PII entities detection job	Write	pii-entities-detection-job*		
StopSentimentDetectionJob	Grants permission to stop a sentiment detection job	Write	sentiment-detection-job*		
StopTargetedSentimentDetectionJob	Grants permission to stop a targeted sentiment detection job	Write	targeted-sentiment-detection-job*		
StopTrainingDocumentClassifier	Grants permission to stop a previously created document classifier training job	Write	document-classifier*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopTrainingEntityRecognizer	Grants permission to stop a previously created entity recognizer training job	Write	entity-recognizer*		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource with given key	Tagging	document-classification-job		
			document-classifier		
			document-classifier-endpoint		
			dominant-language-detection-job		
			entities-detection-job		
			entity-recognizer		
			entity-recognizer-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			events-detection-job		
			flywheel		
			flywheel-dataset		
			key-phrases-detection-job		
			pii-entities-detection-job		
			sentiment-detection-job		
			targeted-sentiment-detection-job		
			topics-detection-job		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEndpoint	Grants permission to update information about the specified endpoint	Write	document-classifier-endpoint*		
			entity-recognizer-endpoint*		
			flywheel		
UpdateFlywheel	Grants permission to Update a flywheel's configuration	Write	flywheel*	comprehend:VolumeKmsKey comprehend:ModelKmsKey comprehend:VpcSecurityGroupIds comprehend:VpcSubnets	
			document-classifier		
			entity-recognizer		

Resource types defined by Amazon Comprehend

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
targeted-sentiment-detection-job	`arn:${Partition}:comprehend:${Region}:${Account}:targeted-sentiment-detection-job/${JobId}`	aws:ResourceTag/${TagKey}
document-classifier	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier/${DocumentClassifierName}`	aws:ResourceTag/${TagKey}
document-classifier-endpoint	`arn:${Partition}:comprehend:${Region}:${Account}:document-classifier-endpoint/${DocumentClassifierEndpointName}`	aws:ResourceTag/${TagKey}
entity-recognizer	`arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer/${EntityRecognizerName}`	aws:ResourceTag/${TagKey}
entity-recognizer-endpoint	`arn:${Partition}:comprehend:${Region}:${Account}:entity-recognizer-endpoint/${EntityRecognizerEndpointName}`	aws:ResourceTag/${TagKey}
dominant-language-detection-job	`arn:${Partition}:comprehend:${Region}:${Account}:dominant-language-detection-job/${JobId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
pii-entities-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:pii-entities-detection-job/${JobId}	aws:ResourceTag/${TagKey}
events-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:events-detection-job/${JobId}	aws:ResourceTag/${TagKey}
key-phrases-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:key-phrases-detection-job/${JobId}	aws:ResourceTag/${TagKey}
sentiment-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:sentiment-detection-job/${JobId}	aws:ResourceTag/${TagKey}
topics-detection-job	arn:${Partition}:comprehend:${Region}:${Account}:topics-detection-job/${JobId}	aws:ResourceTag/${TagKey}
document-classification-job	arn:${Partition}:comprehend:${Region}:${Account}:document-classification-job/${JobId}	aws:ResourceTag/${TagKey}
flywheel	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}	aws:ResourceTag/${TagKey}
flywheel-dataset	arn:${Partition}:comprehend:${Region}:${Account}:flywheel/${FlywheelName}/dataset/${DatasetName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Comprehend

Amazon Comprehend defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by requiring tag values present in a resource creation request	String
aws:ResourceTag/${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
comprehend:DataLakeKmsKey	Filters access by the DataLake Kms Key associated with the flywheel resource in the request	ARN
comprehend:FlywheelIterationId	Filters access by particular Iteration Id for a flywheel	String
comprehend:ModelKmsKey	Filters access by the model KMS key associated with the resource in the request	ARN
comprehend:OutputKmsKey	Filters access by the output KMS key associated with the resource in the request	ARN
comprehend:VolumeKmsKey	Filters access by the volume KMS key associated with the resource in the request	ARN

Condition keys	Description	Type
comprehend:VpcSecurityGroupIds	Filters access by the list of all VPC security group ids associated with the resource in the request	ArrayOfString
comprehend:VpcSubnets	Filters access by the list of all VPC subnets associated with the resource in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Comprehend Medical

Amazon Comprehend Medical (service prefix: `comprehendmedical`) 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 Comprehend Medical
- Resource types defined by Amazon Comprehend Medical
- Condition keys for Amazon Comprehend Medical

Actions defined by Amazon Comprehend Medical

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEntitiesDetectionV2Job	Grants permission to describe the properties of a medical entity detection job that you have submitted	Read			
DescribeICD10CMInferenceJob	Grants permission to describe the properties of an ICD-10-CM linking job that you have submitted	Read			
DescribePHIDetectionJob	Grants permission to describe the properties of a PHI entity detection job that you have submitted	Read			
DescribeRxNormInferenceJob	Grants permission to describe the properties of an RxNorm linking job that you have submitted	Read			
DescribeSNOMEDCTInferenceJob	Grants permission to describe the properties of a SNOMED-CT linking job that you have submitted	Read			
DetectEntitiesV2	Grants permission to detect the named medical entities, and their relationships and traits within the given text document	Read			
DetectPHI	Grants permission to detect the protected health	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	information (PHI) entities within the given text document				
InferICD10CM	Grants permission to detect the medical condition entities within the given text document and link them to ICD-10-CM codes	Read			
InferRxNorm	Grants permission to detect the medication entities within the given text document and link them to RxCUI concept identifiers from the National Library of Medicine RxNorm database	Read			
InferSNOMEDCT	Grants permission to detect the medical condition, anatomy, and test, treatment, and procedure entities within the given text document and link them to SNOMED-CT codes	Read			
ListEntitiesDetectionV2Jobs	Grants permission to list the medical entity detection jobs that you have submitted	Read			
ListICD10CMInferenceJobs	Grants permission to list the ICD-10-CM linking jobs that you have submitted	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPHIDetectionJobs	Grants permission to list the PHI entity detection jobs that you have submitted	Read			
ListRxNormInferenceJobs	Grants permission to list the RxNorm linking jobs that you have submitted	Read			
ListSNOMEDCTInferenceJobs	Grants permission to list the SNOMED-CT linking jobs that you have submitted	Read			
StartEntitiesDetectionV2Job	Grants permission to start an asynchronous medical entity detection job for a collection of documents	Write			
StartICD10CMInferenceJob	Grants permission to start an asynchronous ICD-10-CM linking job for a collection of documents	Write			
StartPHIDetectionJob	Grants permission to start an asynchronous PHI entity detection job for a collection of documents	Write			
StartRxNormInferenceJob	Grants permission to start an asynchronous RxNorm linking job for a collection of documents	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSNOMEDCTInferenceJob	Grants permission to start an asynchronous SNOMED-CT linking job for a collection of documents	Write			
StopEntitiesDetectionV2Job	Grants permission to stop a medical entity detection job	Write			
StopICD10CMInferenceJob	Grants permission to stop an ICD-10-CM linking job	Write			
StopPHIDetectionJob	Grants permission to stop a PHI entity detection job	Write			
StopRxNormInferenceJob	Grants permission to stop an RxNorm linking job	Write			
StopSNOMEDCTInferenceJob	Grants permission to stop a SNOMED-CT linking job	Write			

Resource types defined by Amazon Comprehend Medical

Amazon Comprehend Medical does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Comprehend Medical, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Comprehend Medical

Amazon Comprehend Medical defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Compute Optimizer

AWS 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 AWS Compute Optimizer
- Resource types defined by AWS Compute Optimizer
- Condition keys for AWS Compute Optimizer

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRecommendationPreferences	Grants permission to delete recommendation preferences	Write		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances rds:DescribeDBClusters 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:GetAutoSc

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					alingGroupRecommendations
ExportEBSVolumeRecommendations	Grants permission to export EBS volume recommendations to S3 for the provided accounts	Write			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes
ExportEC2InstanceRecommendations	Grants permission to export EC2 instance recommendations to S3 for the provided accounts	Write			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Compute Optimizer

AWS Compute Optimizer does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Compute Optimizer, specify `"Resource": "*"` in your policy.

Condition keys for AWS Compute Optimizer

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
compute-optimizer:ResourceType	Filters access by the resource type	String

Actions, resources, and condition keys for AWS Compute Optimizer Automation

AWS Compute Optimizer Automation (service prefix: `aco-automation`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Compute Optimizer Automation

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAccounts	Grants permission to associate member accounts with the management account	Write			
CreateAutomationRule	Grants permission to create automation rule	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAutomationRule	Grants permission to delete automation rule	Write	AutomationRule*	aws:ResourceTag/${TagKey}	
DisassociateAccounts	Grants permission to disassociate member accounts from the management account	Write			
GetAutomationEvent	Grants permission to get automation event details	Read			
GetAutomationRule	Grants permission to get automation rule	Read	AutomationRule*	aws:ResourceTag/${TagKey}	
GetEnrollmentConfiguration	Grants permission to get enrollment configuration	Read			
ListAccounts	Grants permission to list the accounts in your organization that are enrolled in Compute Optimizer and whether they have enabled the Automation feature	List			
ListAutomationEventSteps	Grants permission to list automation event steps	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAutomationEventSummaries	Grants permission to list automation event summaries	List			
ListAutomationEvents	Grants permission to list automation events	List			
ListAutomationRulePreview	Grants permission to list automation rule preview results	List			ec2:DescribeVolumes
ListAutomationRulePreviewSummaries	Grants permission to list automation rule preview summaries	List			
ListAutomationRules	Grants permission to list automation rules	List			
ListRecommendedActionSummaries	Grants permission to list recommended action summaries	List			
ListRecommendedActions	Grants permission to list recommended actions	List			ec2:DescribeVolumes
ListTagsForResource	Grants permission to list tags for automation rule	List	AutomationRule*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RollbackAutomationEvent	Grants permission to initiate a rollback for an automation event	Write			
StartAutomationEvent	Grants permission to initiate an on-demand automation for a recommended action	Write			
TagResource	Grants permission to add tags to automation rule	Tagging	AutomationRule*	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from automation rule	Tagging	AutomationRule*	aws:ResourceTag/${TagKey}	
				aws:TagKeys	
UpdateAutomationRule	Grants permission to update automation rule	Write	AutomationRule*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnrollmentConfiguration	Grants permission to update enrollment configuration for the Compute Optimizer automation feature	Write			

Resource types defined by AWS Compute Optimizer Automation

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
AutomationRule	`arn:${Partition}:compute-optimizer::${Account}:automation-rule/${RuleId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Compute Optimizer Automation

AWS Compute Optimizer Automation defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Config

AWS 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 AWS Config
- Resource types defined by AWS Config
- Condition keys for AWS Config

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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 configuration aggregator account in a specified region	Write	AggregationAuthorization*		
DeleteConfigRule	Grants permission to delete the specified AWS Config rule and all of its evaluation results	Write	ConfigRule*		
DeleteConfigurationAggregator	Grants permission to delete the specified configuration aggregator and the aggregate	Write	ConfigurationAggregator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	d data associated with the aggregator				
DeleteConfigurationRecorder	Grants permission to delete the customer managed configuration recorder	Write	ConfigurationRecorder*		
DeleteConformancePack	Grants permission to delete the specified conformance pack and all the AWS 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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Config Rule	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteServiceLinkedConfigurationRecorder	Grants permission to delete the service-linked configuration recorder	Write	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	Grants permission to delete the stored query for an AWS account in an AWS Region	Write	StoredQuery*		
DeliverConfigSnapshot	Grants permission to schedule delivery of a configuration snapshot to the Amazon S3 bucket in the specified delivery channel	Read			
DescribeAggregateComplianceByConfigRules	Grants permission to return a list of compliant and noncompliant rules with the number of resources for compliant and noncompliant rules	Read	ConfigurationAggregator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Config rules are compliant	Read			
DescribeComplianceByResource	Grants permission to indicate whether the specified AWS resources are compliant	Read			
DescribeConfigRuleEvaluationStatus	Grants permission to return status information for each of your AWS managed Config rules	Read			
DescribeConfigRules	Grants permission to return details about your AWS Config rules	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
DescribeConfigurationRecorders	Grants permission to return the names of one or more specified configuration recorders	Read	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Config rule for a specific resource in a rule	Read	ConfigurationAggregator*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAggregateDiscoveredResourceCounts	Grants permission to return the resource counts across accounts and regions that are present in your AWS 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 AWS Config rule	Read	ConfigRule*		
GetComplianceDetailsByResource	Grants permission to return the evaluation results for the specified AWS resource	Read			
GetComplianceSummaryByConfigRule	Grants permission to return the number of AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConformancePackComplianceDetails	Grants permission to return compliance details of a conformance pack for all AWS 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 AWS Config Custom Policy rule	Read	ConfigRule*		
GetDiscoveredResourceCounts	Grants permission to return the resource types, the number of each resource type, and the total number of resources that AWS Config is recording in this region for your AWS account	Read			
GetOrganizationConfigRuleDetailedStatus	Grants permission to return detailed status for each member account within an organization for a given organization config rule	Read	OrganizationConfigRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Config Custom Policy rule	Read	OrganizationConfigRule*		
GetResourceConfigHistory	Grants permission to return a list of configuration items for the specified resource	Read			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfigurationRecorders	Grants permission to list the configuration recorder summaries for an AWS account in an AWS 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			
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 AWS account in an AWS Region	List			
ListStoredQueries	Grants permission to list the stored queries for an AWS account in an AWS Region	List			
ListTagsForResource	Grants permission to list the tags for AWS Config resource	Read	AggregationAuthorization		
			ConfigRule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigRule	Grants permission to add or update an AWS Config rule for evaluating whether your AWS resources comply with your desired configurations	Write	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationAggregator	Grants permission to create and update the configuration aggregator with the selected source accounts and regions	Write	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEvaluations	Grants permission to be used by an AWS Lambda function to deliver evaluation results to AWS Config	Write			
PutExternalEvaluation	Grants permission to deliver evaluation result to AWS Config	Write	ConfigRule*		
PutOrganizationConfigRule	Grants permission to add or update organization config rule for your entire organization evaluating whether your AWS 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 AWS 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 AWS 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 AWS 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 AWS 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 AWS 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 AWS resources you have selected to record in your AWS account	Write	ConfigurationRecorder*		
StartRemediationExecution	Grants permission to run an on-demand remediation for the specified AWS Config rules against the last known remediation configuration	Write			iam:PassRole
StartResourceEvaluation	Grants permission to evaluate your resource details against the AWS Config rules in your account	Write			cloudformation:DescribeType
StopConfigurationRecorder	Grants permission to the customer managed configuration recorder to stop recording configurations of the AWS resources you have selected to record in your AWS account	Write	ConfigurationRecorder*		
TagResource	Grants permission to associate the specified tags to a resource with the specified resourceArn	Tagging	AggregationAuthorization		
			ConfigRule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to delete specified tags from a resource	Tagging	AggregationAuthorization		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

Resource types defined by AWS 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}	
StoredQuery	arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ConfigurationRecorder	arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Config

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString
config:ConfigurationRecorderServicePrincipal	Filters access by service principal of the configuration recorder	String

Actions, resources, and condition keys for Amazon Connect

Amazon Connect (service prefix: 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 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateEvaluationForm	Grants permission to activate an evaluation form in the specified Amazon Connect instance. After the evaluation form is activated, it is available to start new evaluations based on the form	Write	evaluation-form*		
				connect:InstanceId	
AdminGetEmergencyAccessToken	Grants permission to federate into an Amazon Connect instance (Log in for emergency access functiona	Write	instance*		connect:DescribeInstance

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	lity in the Amazon Connect console)				connect:ListInstances ds:DescribeDirectories
Associate Analytics DataSet	Grants permission to grant access and to associate a dataset with the specified AWS account	Write	instance*		
				connect:InstanceId	
Associate ApprovedOrigin	Grants permission to associate approved origin for an existing Amazon Connect instance	Write	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateBot	Grants permission to associate a Lex bot for an existing Amazon Connect instance	Write	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:CreateResourcePolicy lex:DescribeBotAlias lex:GetBot lex:UpdateResourcePolicy
				connect:InstanceId	
Associate ContactWithUser	Grants permission to associate a contact with a user using the Amazon Connect API	Write	contact*		
			instance*		
			user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:PreferredUserArn aws:ResourceTag/${TagKey} connect:InstanceId	
Associate CustomerProfilesDomain [permission only]	Grants permission to associate a Customer Profiles domain for an existing Amazon Connect instance	Write	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy profile:GetDomain
Associate DefaultVocabulary	Grants permission to default vocabulary for an existing Amazon Connect instance	Write	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateEmailAddressAlias	Grants permission to associate an alias with an email address resource in an Amazon Connect instance	Write	email-address*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateFlow	Grants permission to associate a resource with a flow in an Amazon Connect instance	Write	contact-flow* wildcard-phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateInstanceStorageConfig	Grants permission to associate instance storage for an existing Amazon Connect instance	Write	instance*		ds:DescribeDirectories firehose:DescribeDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kinesis:DescribeStream kms:CreateGrant kms:DescribeKey s3:GetBucketAcl

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetBucketLocation
				connect:StorageResourceType connect:InstanceId	
Associate LambdaFunction	Grants permission to associate a Lambda function for an existing Amazon Connect instance	Write	instance*		lambda:AddPermission
				connect:InstanceId	
Associate LexBot	Grants permission to associate a Lex bot for an existing Amazon Connect instance	Write	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:GetBot
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociatePhoneNumberContactFlow	Grants permission to associate contact flow resources to phone number resources in an Amazon Connect instance	Write	contact-flow*		
			phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateQueueEmailAddresses	Grants permission to associate a set of email addresses with a queue	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateQueueQuickConnects	Grants permission to associate quick connects with a queue in an Amazon Connect instance	Write	queue*		
			quick-connect*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateRoutingProfileQueues	Grants permission to associate queues with a routing profile in an Amazon Connect instance	Write	queue*		
			routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateSecurityKey	Grants permission to associate a security key for an existing Amazon Connect instance	Write	instance*		
				connect:InstanceId	
AssociateSecurityProfiles	Grants permission to associate security profiles with an AI agent in an Amazon Connect instance	Write	instance*		
			security-profile*		
			ai-agent		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
AssociateTrafficDistributionGroupUser	Grants permission to associate a user to a traffic distribution group in the specified Amazon Connect instance	Write	instance*		connect:DescribeUser connect:SearchUsers
			traffic-distribution-group*		
			user*		
				connect:InstanceId aws:ResourceTag/${TagKey} connect:SearchTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateUserProficiencies	Grants permission to associate user proficiencies to a user in an Amazon Connect instance	Write	instance*		
			user*		
				connect:InstanceId	
AssociateWorkspace	Grants permission to associate a workspace with a user or routing profile in an Amazon Connect instance	Write	workspace*		
			routing-profile		
			user		
				aws:ResourceTag/${TagKey} connect:InstanceId	
BatchAssociateAnalyticsDataSet	Grants permission to grant access and to associate the datasets with the specified AWS account	Write	instance*		
				connect:InstanceId	
BatchCreateDataTableValue	Grants permission to batch create values in a data table in an Amazon Connect instance	Write	data-table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ExpressionValue connect:PrimaryAttribute/${PrimaryAttribute}	
BatchDeleteDataTableValue	Grants permission to batch delete values in a data table in an Amazon Connect instance	Write	data-table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:PrimaryAttribute/${PrimaryAttribute}	
BatchDescribeDataTableValue	Grants permission to batch describe values in a data table in an Amazon Connect instance	Read	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:PrimaryAttribute/${PrimaryAttribute}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDisassociateAnalyticsDataSet	Grants permission to revoke access and to disassociate the datasets with the specified AWS account	Write	instance*		
				connect:InstanceId	
BatchGetAttachedFileMetadata	Grants permission to get metadata for multiple attached files from an Amazon Connect instance	Read	attached-file*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
BatchGetFlowAssociation	Grants permission to get summary information about the flow associations for the specified Amazon Connect instance	List	wildcard-phone-number*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
BatchPutContact	Grants permission to put contacts in an Amazon Connect instance	Write	instance*		
			queue		
				connect:InstanceId	
BatchUpdateDataTableValue	Grants permission to batch update values in a data table in an Amazon Connect instance	Write	data-table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ExpressionValue connect:PrimaryAttribute/${PrimaryAttribute}	
ClaimPhoneNumber	Grants permission to claim phone number resources in an Amazon Connect instance or traffic distribution group	Write	instance*		
			traffic-distribution-group*		
			wildcard-phone-number*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CompleteAttachedFileUpload	Grants permission to complete an attached file upload in an Amazon Connect instance	Write	attached-file*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateAgentStatus	Grants permission to create agent status in an Amazon Connect instance	Write	agent-status*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateAuthenticationProfile	Grants permission to create authentication profile resources in an Amazon Connect instance	Write	authentication-profile*		
				connect:InstanceId	
CreateContact	Grants permission to create a new contact using the Amazon Connect API	Write	instance*		
			contact		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactInitiationMethod	
CreateContactFlow	Grants permission to create a contact flow in an Amazon Connect instance	Write	contact-flow*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId connect:FlowType	
CreateContactFlowModule	Grants permission to create a contact flow module in an Amazon Connect instance	Write	contact-flow-module*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateContactFlowModuleAlias	Grants permission to create an alias of a flow module version in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
CreateContactFlowModuleVersion	Grants permission to create a version of a flow module in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContactFlowVersion	Grants permission to create a version a flow in an Amazon Connect instance	Write	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
CreateDataTable	Grants permission to create a dataTable in an Amazon Connect instance	Write	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
CreateDataTableAttribute	Grants permission to create an attribute for a data table in an Amazon Connect instance	Write	data-table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
CreateEmailAddress	Grants permission to create an email address resource in an Amazon Connect instance	Write	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateEvaluationForm	Grants permission to create an evaluation form in the specified Amazon Connect instance. The form can be used to define questions related to agent performance, and create sections to organize such questions. Question and section identifiers cannot be duplicated within the same evaluation form	Write	evaluation-form*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHoursOfOperation	Grants permission to create hours of operation in an Amazon Connect instance	Write	hours-of-operation*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateHoursOfOperationOverride	Grants permission to create an hours of operation override in an Amazon Connect instance	Write	hours-of-operation*		
			instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstance	Grants permission to create a new Amazon Connect instance	Write		aws:RequestTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:CheckAlias ds:CreateAlias ds:CreateDirectory ds:CreateIdentityPoolDirectory ds:DeleteDirectory ds:DescribeDirectories ds:UnauthorizeApplication iam:AttachRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole iam:PutRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIntegrationAssociation	Grants permission to create an integration association with an Amazon Connect instance	Write	instance*		app-integrations:CreateApplicationAssociation app-integrations:CreateEventIntegrationAssociation app-integrations:GetApplication app-integrations:GetDataIntegration app-integrations:ListDataIntegration

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					Associations app-integrations:TagResource cases:GetDomain chime:AssociateVoiceConnectorConnect chime:DisassociateVoiceConnectorConnect chime:TagResource chime:UntagResource connect:DescribeInstance

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ds:DescribeDirectories events:PutRule events:PutTargets iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy mobiletargeting:GetApp voiceid:DescribeDomain wisdom:GetAssistant

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					wisdom:GetKnowledgeBase wisdom:TagResource
			integration-association*		
				connect:InstanceId aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotification	Grants permission to create a notification in an Amazon Connect instance	Write	instance*		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateParticipant	Grants permission to add a participant to an ongoing contact	Write	contact* instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
CreatePersistentContactAssociation	Grants permission to create persistent contact associations for a contact	Write	contact* instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePredefinedAttribute	Grants permission to create a predefined attribute in an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
CreatePrompt	Grants permission to create a prompt in an Amazon Connect instance	Write	prompt*		kms:Decrypt s3:GetObject s3:GetObjectAcl
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreatePushNotificationRegistration	Grants permission to create a push notification registration for an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
CreateQueue	Grants permission to create a queue in an Amazon Connect instance	Write	hours-of-operation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			queue*		
			contact-flow		
			phone-number		
			quick-connect		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateQuickConnect	Grants permission to create a quick connect in an Amazon Connect instance	Write	quick-connect*		
			contact-flow		
			queue		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateRoutingProfile	Grants permission to create a routing profile in an Amazon Connect instance	Write	queue*		
			routing-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateRule	Grants permission to create a rule in an Amazon Connect instance	Write	rule*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSecurityProfile	Grants permission to create a security profile for the specified Amazon Connect instance	Write	security-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateTaskTemplate	Grants permission to create a task template in an Amazon Connect instance	Write	task-template*		
CreateTrafficDistributionGroup	Grants permission to create a traffic distribution group	Write	instance*		
			traffic-distribution-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateUseCase	Grants permission to create a use case for an integration association	Write	instance*		connect:DescribeInstance ds:DescribeDirectories
			integration-association*		
			use-case*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Grants permission to create a user for the specified Amazon Connect instance	Write	routing-profile*		
			security-profile*		
			user*		
			hierarchy-group		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUserHierarchyGroup	Grants permission to create a user hierarchy group in an Amazon Connect instance	Write	hierarchy-group		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateView	Grants permission to create a view in an Amazon Connect instance	Write	customer-managed-view*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateViewVersion	Grants permission to create a view version in an Amazon Connect instance	Write	customer-managed-view*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
CreateVocabulary	Grants permission to create a vocabulary in an Amazon Connect instance	Write	vocabulary*		
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateWorkspace	Grants permission to create a workspace in an Amazon Connect instance	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
CreateWorkspacePage	Grants permission to create a workspace page in an Amazon Connect instance	Write	workspace* aws-managed-view customer-managed-view		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeactivateEvaluationForm	Grants permission to deactivate an evaluation form in the specified Amazon Connect instance. After a form is deactivated, it is no longer available for users to start new evaluations based on the form	Write	evaluation-form*		
				connect:InstanceId	
DeleteAttachedFile	Grants permission to delete an attached file from an Amazon Connect instance	Write	attached-file*		cases:DeleteRelatedItem
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
DeleteContactEvaluation	Grants permission to delete a contact evaluation in the specified Amazon Connect instance	Write	contact-evaluation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteContactFlow	Grants permission to delete a contact flow in an Amazon Connect instance	Write	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
DeleteContactFlowModule	Grants permission to delete a contact flow module in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContactFlowModuleAlias	Grants permission to delete an alias of a flow module version in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteContactFlowModuleVersion	Grants permission to delete a version of a flow module in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteContactFlowVersion	Grants permission to delete a version of a flow in an Amazon Connect instance	Write	contact-flow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
DeleteDataTable	Grants permission to delete a data table in an Amazon Connect instance	Write	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteDataTableAttribute	Grants permission to delete an attribute of a data table in an Amazon Connect instance	Write	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEmailAddress	Grants permission to delete an email address resource in an Amazon Connect instance	Write	email-address*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteEvaluationForm	Grants permission to delete an evaluation form in the specified Amazon Connect instance. If the version property is provided, only the specified version of the evaluation form is deleted	Write	evaluation-form*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteHoursOfOperation	Grants permission to delete hours of operation in an Amazon Connect instance	Write	hours-of-operation*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteHoursOfOperationOverride	Grants permission to delete an hours of operation override in an Amazon Connect instance	Write	hours-of-operation*		
			instance*		
				connect:InstanceId	
DeleteInstance	Grants permission to delete an Amazon Connect instance. When you remove an instance, the link to an existing AWS directory is also removed	Write	instance*		ds:DeleteDirectory ds:DescribeDirectories ds:UnauthorizeApplication
				connect:InstanceId aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIntegrationAssociation	Grants permission to delete an integration association from an Amazon Connect instance. The association must not have any use cases associated with it	Write	instance*		app-integrations:DeleteApplicationAssociation app-integrations:DeleteEventIntegrationAssociation app-integrations:UntagResource connect:DescribeInstance ds:DescribeDirectories events:DeleteRule

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					events:ListTargetsByRule events:RemoveTargets
			integration-association*		
				connect:InstanceId	
DeleteNotification	Grants permission to delete a notification in an Amazon Connect instance	Write	notification*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeletePredefinedAttribute	Grants permission to delete a predefined attribute in an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
DeletePrompt	Grants permission to delete a prompt in an Amazon Connect instance	Write	prompt*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeletePushNotificationRegistration	Grants permission to delete a push notification registration for an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
DeleteQueue	Grants permission to delete a queue in an Amazon Connect instance	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteQuickConnect	Grants permission to delete a quick connect in an Amazon Connect instance	Write	quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoutingProfile	Grants permission to delete routing profiles in an Amazon Connect instance	Write	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteRule	Grants permission to delete a rule in an Amazon Connect instance	Write	rule*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteSecurityProfile	Grants permission to delete a security profile in an Amazon Connect instance	Write	security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTaskTemplate	Grants permission to delete a task template in an Amazon Connect instance	Write	task-template*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteTrafficDistributionGroup	Grants permission to delete a traffic distribution group	Write	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
DeleteUseCase	Grants permission to delete a use case from an integration association	Write	instance*		connect:DescribeInstance ds:DescribeDirectories
			use-case*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUser	Grants permission to delete a user in an Amazon Connect instance	Write	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteUserHierarchyGroup	Grants permission to delete a user hierarchy group in an Amazon Connect instance	Write	hierarchy-group*		
				connect:InstanceId	
DeleteView	Grants permission to delete a view in an Amazon Connect instance	Write	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteViewVersion	Grants permission to delete a view version in an Amazon Connect instance	Write	customer-managed-view-version*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteVocabulary	Grants permission to delete a vocabulary in an Amazon Connect instance	Write	vocabulary*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteWorkspace	Grants permission to delete a workspace in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteWorkspaceMedia	Grants permission to delete workspace media in an Amazon Connect instance	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DeleteWorkspacePage	Grants permission to delete a workspace page in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeAgentStatus	Grants permission to describe agent status in an Amazon Connect instance	Read	agent-status*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeAuthenticationProfile	Grants permission to describe authentication profile resources in an Amazon Connect instance	Read	authentication-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId	
DescribeContact	Grants permission to describe a contact in an Amazon Connect instance	Read	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
DescribeContactEvaluation	Grants permission to describe a contact evaluation in the specified Amazon Connect instance	Read	contact-evaluation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeContactFlow	Grants permission to describe a contact flow in an Amazon Connect instance	Read	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
DescribeContactFlowModule	Grants permission to describe a contact flow module in an Amazon Connect instance	Read	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeContactFlowModuleAlias	Grants permission to describe an alias of a flow module version in an Amazon Connect instance	Read	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeDataTable	Grants permission to describe a data table in an Amazon Connect instance	Read	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeDataTableAttribute	Grants permission to describe an attribute of a data table in an Amazon Connect instance	Read	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEmailAddress	Grants permission to describe an email address resource in an Amazon Connect instance	Read	email-address*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeEvaluationForm	Grants permission to describe an evaluation form in the specified Amazon Connect instance. If the version property is not provided, the latest version of the evaluation form is described	Read	evaluation-form*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeForecastingPlanningSchedulingIntegration [permission only]	Grants permission to describe the status of forecasting, planning, and scheduling integration on an Amazon Connect instance	Read	instance*		
				connect:InstanceId	
DescribeHoursOfOperation	Grants permission to describe hours of operation in an Amazon Connect instance	Read	hours-of-operation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeHoursOfOperationOverride	Grants permission to describe an hours of operation override in an Amazon Connect instance	Read	hours-of-operation*		
			instance*		
				connect:InstanceId	
DescribeInstance	Grants permission to view details of an Amazon Connect instance and is also required to create an instance	Read	instance*		ds:DescribeDirectories
				connect:InstanceId aws:ResourceTag/${TagKey}	
DescribeInstanceAttribute	Grants permission to view the attribute details of an existing Amazon Connect instance	Read	instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:AttributeType connect:InstanceId	
DescribeInstanceStorageConfig	Grants permission to view the instance storage configuration for an existing Amazon Connect instance	Read	instance*		
				connect:StorageResourceType connect:InstanceId	
DescribeNotification	Grants permission to describe a notification in an Amazon Connect instance	Read	notification*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribePhoneNumber	Grants permission to describe phone number resources in an Amazon Connect instance or traffic distribution group	Read	phone-number*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePredefinedAttribute	Grants permission to describe a predefined attribute in an Amazon Connect instance	Read	instance*		
				connect:InstanceId	
DescribePrompt	Grants permission to describe a prompt in an Amazon Connect instance	Read	prompt*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeQueue	Grants permission to describe a queue in an Amazon Connect instance	Read	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeQuickConnect	Grants permission to describe a quick connect in an Amazon Connect instance	Read	quick-connect*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeRoutingProfile	Grants permission to describe a routing profile in an Amazon Connect instance	Read	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeRule	Grants permission to describe a rule in an Amazon Connect instance	Read	rule*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeSecurityProfile	Grants permission to describe a security profile in an Amazon Connect instance	Read	security-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeTrafficDistributionGroup	Grants permission to describe a traffic distribution group	Read	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
DescribeUser	Grants permission to describe a user in an Amazon Connect instance	Read	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeUserHierarchyGroup	Grants permission to describe a hierarchy group for an Amazon Connect instance	Read	hierarchy-group*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeUserHierarchyStructure	Grants permission to describe the hierarchy structure for an Amazon Connect instance	Read	instance*		
				connect:InstanceId	
DescribeView	Grants permission to describe a view in an Amazon Connect instance		aws-managed-view*		
			customer-managed-view*		
			qualified-aws-managed-view*		
			qualified-customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVocabulary	Grants permission to describe a vocabulary in an Amazon Connect instance	Read	vocabulary*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DescribeWorkspace	Grants permission to describe a workspace in an Amazon Connect instance	Read	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateAnalyticsDataSet	Grants permission to revoke access and to disassociate a dataset with the specified AWS account	Write	instance*		
				connect:InstanceId	
DisassociateApprovedOrigin	Grants permission to disassociate approved origin for an existing Amazon Connect instance	Write	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateBot	Grants permission to disassociate a Lex bot for an existing Amazon Connect instance	Write	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy lex:DeleteResourcePolicy lex:UpdateResourcePolicy
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateCustomerProfilesDomain [permission only]	Grants permission to disassociate a Customer Profiles domain for an existing Amazon Connect instance	Write	instance*		iam:AttachRolePolicy iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetPolicy iam:GetPolicyVersion iam:GetRolePolicy
DisassociateEmailAddressAlias	Grants permission to disassociate an alias from an email address resource in an Amazon Connect instance	Write	email-address*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateFlow	Grants permission to disassociate a resource from a flow in an Amazon Connect instance	Write	wildcard-phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateInstanceStorageConfig	Grants permission to disassociate instance storage for an existing Amazon Connect instance	Write	instance*		
				connect:StorageResourceType connect:InstanceId	
DisassociateLambdaFunction	Grants permission to disassociate a Lambda function for an existing Amazon Connect instance	Write	instance*		lambda:RemovePermission
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateLexBot	Grants permission to disassociate a Lex bot for an existing Amazon Connect instance	Write	instance*		iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy
				connect:InstanceId	
DisassociatePhoneNumberContactFlow	Grants permission to disassociate contact flow resources from phone number resources in an Amazon Connect instance	Write	phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateQueueEmailAddresses	Grants permission to disassociate a set of email addresses from a queue	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateQueueQuickConnects	Grants permission to disassociate quick connects from a queue in an Amazon Connect instance	Write	queue*		
			quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateRoutingProfileQueues	Grants permission to disassociate queues from a routing profile in an Amazon Connect instance	Write	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateSecurityKey	Grants permission to disassociate the security key for an existing Amazon Connect instance	Write	instance*		
				connect:InstanceId	
DisassociateSecurityProfiles	Grants permission to disassociate security profiles with an AI agent in an Amazon Connect instance	Write	instance*		
			security-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ai-agent		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DisassociateTrafficDistributionGroupUser	Grants permission to disassociate a user from a traffic distribution group in the specified Amazon Connect instance	Write	instance*		
			traffic-distribution-group*		
			user*		
				connect:InstanceId aws:ResourceTag/${TagKey}	
DisassociateUserProficiencies	Grants permission to disassociate user proficiencies from a user in an Amazon Connect instance	Write	instance*		
			user*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateWorkspace	Grants permission to disassociate a workspace from a user or routing profile in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
DismissUserContact	Grants permission to dismiss terminated Contact from Agent CCP	Write	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
EvaluateDataTableValues	Grants permission to evaluate values in a data table in an Amazon Connect instance	Read	data-table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:PrimaryAttribute/${PrimaryAttribute}	
GetAttachedFile	Grants permission to get an attached file from an Amazon Connect instance	Read	attached-file*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContactAttributes	Grants permission to retrieve the contact attributes for the specified contact	Read	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
GetContactMetrics	Grants permission to get contact metrics in an Amazon Connect instance	Read	contact*		
			instance*		
				connect:InstanceId	
GetCurrentMetricData	Grants permission to retrieve current metric data for queues and routing profiles in an Amazon Connect instance	Read	queue*		
			routing-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetCurrentUserData	Grants permission to retrieve current user data in an Amazon Connect instance	Read	hierarchy-group*		
			queue*		
			routing-profile*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetEffectiveHoursOfOperations	Grants permission to get effective hours of operation resources in an Amazon Connect instance	Read	hours-of-operation*		
			instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFederationToken	Grants permission to federate into an Amazon Connect instance when using SAML-based authentication for identity management	Read	instance*		
				connect:InstanceId	
GetFlowAssociation	Grants permission to get information about the flow associations for the specified Amazon Connect instance	Read	wildcard-phone-number*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetMetricData	Grants permission to retrieve historical metric data for queues in an Amazon Connect instance	Read	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetMetricDataV2	Grants permission to retrieve metric data in an Amazon Connect instance	Read	hierarchy-group*		
			queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			routing-profile*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetPromptFile	Grants permission to get details about a prompt's presigned Amazon S3 URL in an Amazon Connect instance	Read	prompt*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
GetTaskTemplate	Grants permission to get details about specified task template in an Amazon Connect instance	Read	task-template*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrafficDistribution	Grants permission to read traffic distribution for a traffic distribution group	List	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
ImportPhoneNumber	Grants permission to import phone number resources to an Amazon Connect instance	Write	instance*		sms-voice:DescribePhoneNumbers social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber social-messaging:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			wildcard-phone-number*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportWorkspaceMedia	Grants permission to import workspace media in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListAgentStatuses	Grants permission to list agent statuses in an Amazon Connect instance	List	wildcard-agent-status*		
ListAnalyticsDataAssociations	Grants permission to list the association status of a dataset for a given Amazon Connect instance	List	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAnalyticsDataLakeDataSets	Grants permission to list data lake datasets available to associate with for a given Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListApprovedOrigins	Grants permission to view approved origins of an existing Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListAssociatedContacts	Grants permission to list the contacts associated with an email address in an Amazon Connect instance	List	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListAuthenticationProfiles	Grants permission to list authentication profile resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListBots	Grants permission to view the Lex bots of an existing Amazon Connect instance	List	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContactEvaluations	Grants permission to list contact evaluations in the specified Amazon Connect instance	List	instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListContactFlowModuleAliases	Grants permission to list the aliases of a flow module in an Amazon Connect instance	List	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListContactFlowModuleVersions	Grants permission to list all the versions of a flow module in an Amazon Connect instance	List	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContactFlowModules	Grants permission to list contact flow module resources in an Amazon Connect instance	List	instance*		
ListContactFlowVersions	Grants permission to list all the versions a flow in an Amazon Connect instance	List	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
ListContactFlows	Grants permission to list contact flow resources in an Amazon Connect instance	List	wildcard-contact-flow*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContactReferences	Grants permission to list references associated with a contact in an Amazon Connect instance	List	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
ListDataTableAttributes	Grants permission to list attributes of a data table in an Amazon Connect instance	List	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataTablePrimaryValues	Grants permission to list primary values in a data table in an Amazon Connect instance	List	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:PrimaryAttribute/${PrimaryAttribute}	
ListDataTableValues	Grants permission to list values in a data table in an Amazon Connect instance	List	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:PrimaryAttribute/${PrimaryAttribute}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataTables	Grants permission to list data tables in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListDefaultVocabularies	Grants permission to list default vocabularies associated with a Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListEntitySecurityProfiles	Grants permission to list security profiles associated with an entity in an Amazon Connect instance	List	instance*		
			ai-agent		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListEvaluationFormVersions	Grants permission to list versions of an evaluation form in the specified Amazon Connect instance	List	evaluation-form*		
				connect:InstanceId	
ListEvaluationForms	Grants permission to list evaluation forms in the specified Amazon Connect instance	List	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFlowAssociations	Grants permission to list summary information about the flow associations for the specified Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListHoursOfOperationOverrides	Grants permission to list hours of operation override resources in an Amazon Connect instance	List	hours-of-operation*		
			instance*		
				connect:InstanceId	
ListHoursOfOperations	Grants permission to list hours of operation resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListInstanceAttributes	Grants permission to view the attributes of an existing Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListInstanceStorageConfigs	Grants permission to view storage configurations of an existing Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListInstances	Grants permission to view the Amazon Connect instances associated with an AWS account	List			ds:DescribeDirectories

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIntegrationAssociations	Grants permission to list summary information about the integration associations for the specified Amazon Connect instance	List	instance*		connect:DescribeInstance ds:DescribeDirectories
				connect:InstanceId	
ListLambdaFunctions	Grants permission to view the Lambda functions of an existing Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListLexBots	Grants permission to view the Lex bots of an existing Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListNotifications	Grants permission to list notifications in an Amazon Connect instance	Read	instance*		
				connect:InstanceId	
ListPhoneNumbers	Grants permission to list phone number resources in an Amazon Connect instance	List	wildcard-legacy-phone-number*		
ListPhoneNumbersV2	Grants permission to list phone number resources in an Amazon Connect instance	List	wildcard-phone-number*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPredefinedAttributes	Grants permission to list predefined attributes in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListPrompts	Grants permission to list prompt resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListQueueEmailAddresses	Grants permission to list the email address metadata associated with a queue	List	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListQueueQuickConnects	Grants permission to list quick connect resources in a queue in an Amazon Connect instance	List	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListQueues	Grants permission to list queue resources in an Amazon Connect instance	List	wildcard-queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListQuickConnects	Grants permission to list quick connect resources in an Amazon Connect instance	List	wildcard-quick-connect*		
ListRealtimeContactAnalysisSegments	Grants permission to list the analysis segments for a real-time analysis session	Read	contact*		
				aws:ResourceTag/${TagKey}	
ListRealtimeContactAnalysisSegmentsV2	Grants permission to list the analysis segments for a real-time chat analytics session	List	contact*		
				aws:ResourceTag/${TagKey} connect:ListRealtimeContactAnalysisSegmentsByOutputType connect:ListRealtimeContactAnalysisSegmentsBySegmentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRoutingProfileManualAssignmentQueues	Grants permission to list manual assignment queue resources in a routing profile in an Amazon Connect instance	List	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListRoutingProfileQueues	Grants permission to list queue resources in a routing profile in an Amazon Connect instance	List	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListRoutingProfiles	Grants permission to list routing profile resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListRules	Grants permission to list rules associated with a Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListSecurityKeys	Grants permission to view the security keys of an existing Amazon Connect instance	List	instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId	
ListSecurityProfileApplications	Grants permission to list applications associated with a specific security profile in an Amazon Connect instance	List	security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListSecurityProfileFlowModules	Grants permission to list flow modules associated with a security profile in an Amazon Connect instance	List	instance*		
			security-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListSecurityProfilePermissions	Grants permission to list permissions associated with security profile in an Amazon Connect instance	List	security-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListSecurityProfiles	Grants permission to list security profile resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListTagsForResource	Grants permission to list tags for an Amazon Connect resource	Read	agent-status		
			contact-evaluation		
			contact-flow		
			contact-flow-module		
			evaluation-form		
			hierarchy-group		
			hours-of-operation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integration-association		
			phone-number		
			prompt		
			queue		
			quick-connect		
			routing-profile		
			rule		
			security-profile		
			traffic-distribution-group		
			use-case		
			user		
			wildcard-phone-number		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListTaskTemplates	Grants permission to list task template resources in an Amazon Connect instance	List	instance*		
ListTrafficDistributionGroupUsers	Grants permission to list the active user associations for a traffic distribution group	List	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
ListTrafficDistributionGroups	Grants permission to list traffic distribution groups	List	traffic-distribution-group*		
ListUseCases	Grants permission to list the use cases of an integration association	List	instance*		connect:DescribeInstance ds:DescribeDirectories

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId	
ListUserHierarchyGroups	Grants permission to list the hierarchy group resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListUserNotifications	Grants permission to list notifications for a user in an Amazon Connect instance	Read	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListUserProficiencies	Grants permission to list user proficiencies from a user in an Amazon Connect instance	List	instance*		
			user*		
				connect:InstanceId	
ListUsers	Grants permission to list user resources in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListViewVersions	Grants permission to list the view versions in an Amazon Connect instance	List	aws-managed-view*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListViews	Grants permission to list the views in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
ListWorkspaceMedia	Grants permission to list workspace media in an Amazon Connect instance	List	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListWorkspacePages	Grants permission to list workspace pages in an Amazon Connect instance	List	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
ListWorkspaces	Grants permission to list workspaces in an Amazon Connect instance	List	instance*		
				connect:InstanceId	
MonitorContact	Grants permission to monitor an ongoing contact	Write	contact*		
			instance*		
			user*		
				connect:MonitorCapabilities aws:ResourceTag/${TagKey} connect:InstanceId	
PauseContact	Grants permission to pause an ongoing contact	Write	contact*		
			instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			contact-flow		
				aws:ResourceTag/${TagKey} connect:InstanceId	
PutUserStatus	Grants permission to switch User Status in an Amazon Connect instance	Write	agent-status*		
			instance*		
			user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
ReleasePhoneNumber	Grants permission to release phone number resources in an Amazon Connect instance	Write	phone-number*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Replicate Instance	Grants permission to create a replica of an Amazon Connect instance	Write	instance*		ds:AuthorizeApplication ds:CheckAlias ds:CreateAlias ds:CreateDirectory ds:CreateIdentityPoolDirectory ds:DeleteDirectory ds:DescribeDirectories ds:UnauthorizeApplication iam:AttachRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole iam:PutRolePolicy
				aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId	
ResumeContact	Grants permission to resume a paused contact	Write	contact*		
			instance*		
			contact-flow		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResumeContactRecording	Grants permission to resume recording for the specified contact	Write	contact*		
				aws:ResourceTag/${TagKey} connect:ContactAssociationId connect:Channel connect:UserArn	
SearchAgentStatuses	Grants permission to search agent status resources in an Amazon Connect instance	Read	instance*		connect:DescribeAgentStatus
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchAvailablePhoneNumbers	Grants permission to search phone number resources in an Amazon Connect instance or traffic distribution group	List	wildcard-phone-number*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchContactEvaluations	Grants permission to search evaluation resources in an Amazon Connect instance	Read	instance*		connect:DescribeContactEvaluation
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchContactFlowModules	Grants permission to search contact flow module resources in an Amazon Connect instance	Read	instance*		connect:DescribeContactFlowModule
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchContactFlows	Grants permission to search contact flow resources in an Amazon Connect instance	Read	instance*		connect:DescribeContactFlow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId connect:SearchTag/${TagKey} connect:FlowType	
SearchContacts	Grants permission to search contacts in an Amazon Connect instance	Read	instance*		connect:DescribeContact
				connect:SearchTag/${TagKey} connect:InstanceId connect:SearchContactsByContactAnalysis connect:Channel connect:PreferredUserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchDataTables	Grants permission to search data tables in an Amazon Connect instance	Read	instance*		connect:DescribeDataTable
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchEmailAddresses	Grants permission to search email address resources in an Amazon Connect instance	Read	instance*		connect:DescribeEmailAddress
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchEvaluationForms	Grants permission to search evaluation forms resources in an Amazon Connect instance	Read	instance*		connect:DescribeEvaluationForm
				connect:InstanceId connect:SearchTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchHoursOfOperationOverrides	Grants permission to search hours of operation override resources in an Amazon Connect instance	Read	hours-of-operation*		connect:DescribeHoursOfOperation connect:ListHoursOfOperationOverrides
			instance*		
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchHoursOfOperations	Grants permission to search hours of operation resources in an Amazon Connect instance	Read	instance*		connect:DescribeHoursOfOperation
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchNotifications		Read	instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to search notifications in an Amazon Connect instance			connect:InstanceId connect:SearchTag/${TagKey}	
SearchPredefinedAttributes	Grants permission to search predefined attributes in an Amazon Connect instance	Read	instance*		connect:DescribePredefinedAttribute
				connect:InstanceId	
SearchPrompts	Grants permission to search prompt resources in an Amazon Connect instance	Read	instance*		connect:DescribePrompt
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchQueues	Grants permission to search queue resources in an Amazon Connect instance	Read	instance*		connect:DescribeQueue

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchQuickConnects	Grants permission to search quick connect resources in an Amazon Connect instance	Read	instance*		connect:DescribeQuickConnect
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchResourceTags	Grants permission to search tags that are used in an Amazon Connect instance	List	instance*		
				connect:InstanceId aws:ResourceTag/${TagKey}	
SearchRoutingProfiles	Grants permission to search routing profile resources in an Amazon Connect instance	Read	instance*		connect:DescribeRoutingProfile

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchSecurityProfiles	Grants permission to search security profile resources in an Amazon Connect instance	Read	instance*		connect:DescribeSecurityProfile
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchUserHierarchyGroups	Grants permission to search user hierarchy group resources in an Amazon Connect instance	Read	instance*		connect:DescribeUserHierarchyGroup
				connect:InstanceId connect:SearchTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchUsers	Grants permission to search user resources in an Amazon Connect instance	Read	instance*		connect:DescribeUser connect:ListUserProficiencies
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchViews	Grants permission to search views in an Amazon Connect instance	Read	instance*		connect:DescribeView
				connect:InstanceId connect:SearchTag/${TagKey}	
SearchVocabularies	Grants permission to search vocabularies in a Amazon Connect instance	List	vocabulary*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchWorkspaceAssociations	Grants permission to search workspace associations in an Amazon Connect instance	Read	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
SearchWorkspaces	Grants permission to search workspaces in an Amazon Connect instance	Read	instance*		connect:DescribeWorkspace
				connect:InstanceId connect:SearchTag/${TagKey}	
SendChatIntegrationEvent	Grants permission to send chat integration events using the Amazon Connect API	Write			
SendIntegrationEvent [permission only]	Grants permission to send integration events using the Amazon Connect API	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendOutboundChatMessage [permission only]	Grants permission to send outbound chat messages using the Amazon Connect API	Write	instance*		social-messaging:SendWhatsAppMessage wisdom:GetMessageTemplate wisdom:RenderMessageTemplate
			phone-number*		
				connect:InstanceId connect:Subtype	
SendOutboundEmail	Grants permission to send outbound email using the Amazon Connect API	Write	instance*		
				connect:InstanceId	
StartAttachedFileUpload	Grants permission to start an attached file upload in an Amazon Connect instance	Write	attached-file*		cases:CreateRelatedItem

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys connect:InstanceId connect:UserArn	
StartChatContact	Grants permission to initiate a chat using the Amazon Connect API	Write	contact-flow*		
			contact		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartContactEvaluation	Grants permission to start an empty evaluation in the specified Amazon Connect instance, using the given evaluation form for the particular contact. The evaluation form version used for the contact evaluation corresponds to the currently activated version. If no version is activated for the evaluation form, the contact evaluation cannot be started	Write	contact*		
			contact-evaluation*		
			evaluation-form*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
StartContactMediaProcessing	Grants permission to start message processing on an ongoing contact	Write	contact*		
			instance*		
				connect:InstanceId	
StartContactRecording	Grants permission to start recording for the specified contact	Write	contact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:ContactAssociationId connect:Channel connect:UserArn	
StartContactStreaming	Grants permission to start chat streaming using the Amazon Connect API	Write	instance*		
				aws:ResourceTag/${TagKey}	
StartEmailContact	Grants permission to initiate an inbound email using the Amazon Connect API	Write	contact-flow		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartForecastingPlanningSchedulingIntegration [permission only]	Grants permission to enable forecasting, planning, and scheduling integration on an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
StartOutboundChatContact	Grants permission to initiate an outbound chat using the Amazon Connect API	Write	contact-flow*		wisdom:GetMessageTemplate wisdom:RenderMessageTemplate
			instance*		
			contact		
			phone-number		
				connect:InstanceId connect:Subtype	
StartOutboundEmailContact	Grants permission to initiate an outbound email using the Amazon Connect API	Write	contact-flow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
StartOutboundVoiceContact	Grants permission to initiate outbound calls using the Amazon Connect API	Write	contact*		
StartScreenSharing	Grants permission to start screen sharing for contact	Write	contact* instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTaskContact	Grants permission to initiate a task using the Amazon Connect API	Write	contact-flow*		
			contact		
			quick-connect		
			task-template		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:AssignmentType	
StartWebRTCContact	Grants permission to initiate a WebRTC contact using the Amazon Connect API	Write	contact-flow*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopContact	Grants permission to stop contacts that were initiated using the Amazon Connect API. If you use this operation on an active contact the contact ends, even if the agent is active on a call with a customer	Write	contact*		
				connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
StopContactMediaProcessing	Grants permission to stop message processing on an ongoing contact	Write	contact*		
			instance*		
				connect:InstanceId	
StopContactRecording	Grants permission to stop recording for the specified contact	Write	contact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:ContactAssociationId connect:Channel connect:UserArn	
StopContactStreaming	Grants permission to stop chat streaming using the Amazon Connect API	Write	instance*		
				aws:ResourceTag/${TagKey}	
StopForecastingPlanningSchedulingIntegration [permission only]	Grants permission to disable forecasting, planning, and scheduling integration on an Amazon Connect instance	Write	instance*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SubmitContactEvaluation	Grants permission to submit a contact evaluation in the specified Amazon Connect instance. Answers included in the request are merged with existing answers for the given evaluation. If no answers or notes are passed, the evaluation is submitted with the existing answers and notes. You can delete an answer or note by passing an empty object ({}) to the question identifier	Write	contact-evaluation*		
				connect:InstanceId	
SuspendContactRecording	Grants permission to suspend recording for the specified contact	Write	contact*		
				aws:ResourceTag/${TagKey} connect:ContactAssociationId connect:Channel connect:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagContact	Grants permission to tag a contact in an Amazon Connect instance	Write	contact*		
				aws:TagKeys aws:RequestTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
TagResource	Grants permission to tag an Amazon Connect resource	Tagging	agent-status		
			contact-evaluation		
			contact-flow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			contact-flow-module		
			customer-managed-view		
			email-address		
			evaluation-form		
			hierarchy-group		
			hours-of-operation		
			instance		
			integration-association		
			phone-number		
			prompt		
			queue		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			quick-connect		
			routing-profile		
			rule		
			security-profile		
			task-template		
			traffic-distribution-group		
			use-case		
			user		
			vocabulary		
			wildcard-phone-number		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TransferContact	Grants permission to transfer the contact to another queue or agent	Write	contact*		
			contact-flow*		
			instance*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagContact	Grants permission to untag a contact in an Amazon Connect instance	Write	contact*		
				aws:TagKeys connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
UntagResource	Grants permission to untag an Amazon Connect resource	Tagging	agent-status		
			contact-evaluation		
			contact-flow		
			contact-flow-module		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			customer-managed-view		
			email-address		
			evaluation-form		
			hierarchy-group		
			hours-of-operation		
			instance		
			integration-association		
			phone-number		
			prompt		
			queue		
			quick-connect		
			routing-profile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rule		
			security-profile		
			task-template		
			traffic-distribution-group		
			use-case		
			user		
			vocabulary		
			wildcard-phone-number		
				aws:TagKeys	
UpdateAgentStatus	Grants permission to update agent status in an Amazon Connect instance	Write	agent-status*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateAuthenticationProfile	Grants permission to update authentication profile resources in an Amazon Connect instance	Write	authentication-profile*		
				connect:InstanceId	
UpdateContact	Grants permission to update a contact in an Amazon Connect instance	Write	contact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContactAttributes	Grants permission to create or update the contact attributes associated with the specified contact	Write	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
UpdateContactEvaluation	Grants permission to update details about a contact evaluation in the specified Amazon Connect instance. A contact evaluation must be in the draft state. Answers included in the request are merged with existing answers for the given evaluation. An answer or note can be deleted by passing an empty object ({}) to the question identifier	Write	contact-evaluation*		
				connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContactFlowContent	Grants permission to update contact flow content in an Amazon Connect instance	Write	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
UpdateContactFlowMetadata	Grants permission to update the metadata of a contact flow in an Amazon Connect instance	Write	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
UpdateContactFlowModuleAlias	Grants permission to update an alias of a flow module version in an Amazon Connect instance	Write	contact-flow-module*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateContactFlowModuleContent	Grants permission to update contact flow module content in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateContactFlowModuleMetadata	Grants permission to update the metadata of a contact flow module in an Amazon Connect instance	Write	contact-flow-module*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContactFlowName	Grants permission to update the name and description of a contact flow in an Amazon Connect instance	Write	contact-flow*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:FlowType	
UpdateContactRoutingData	Grants permission to update routing properties on a contact in an Amazon Connect instance	Write	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContactSchedule	Grants permission to update the schedule of a contact that is already scheduled in an Amazon Connect instance	Write	contact*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:ContactAssociationId connect:Channel connect:UserArn	
UpdateDataTableAttribute	Grants permission to update an attribute of a data table in an Amazon Connect instance	Write	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataTableMetadata	Grants permission to update metadata of a data table in an Amazon Connect instance	Write	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateDataTablePrimaryValues	Grants permission to update primary values in a data table in an Amazon Connect instance	Write	data-table*		
				aws:ResourceTag/${TagKey} connect:InstanceId connect:PrimaryAttribute/${PrimaryAttribute}	
UpdateEmailAddressMetadata	Grants permission to update the metadata of an email address resource in an Amazon Connect instance	Write	email-address*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateEvaluationForm	Grants permission to update details about a specific evaluation form version in the specified Amazon Connect instance. Question and section identifiers cannot be duplicated within the same evaluation form	Write	evaluation-form*		
				connect:InstanceId	
UpdateHoursOfOperation	Grants permission to update hours of operation in an Amazon Connect instance	Write	hours-of-operation*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateHoursOfOperationOverride	Grants permission to update an hours of operation override in an Amazon Connect instance	Write	hours-of-operation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*		
				connect:InstanceId	
UpdateInstanceAttribute	Grants permission to update the attribute for an existing Amazon Connect instance	Write	instance*		ds:DescribeDirectories iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy logs:CreateLogGroup
				connect:AttributeType connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceStorageConfig	Grants permission to update the storage configuration for an existing Amazon Connect instance	Write	instance*		ds:DescribeDirectories firehose:DescribeDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kinesis:DescribeStream kms:CreateGrant kms:DescribeKey s3:GetBucketAcl

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetBucketLocation
				connect:StorageResourceType connect:InstanceId	
UpdateNotificationContent	Grants permission to update the content of a notification in an Amazon Connect instance	Write	notification*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateParticipantAuthentication	Grants permission to update and continue authentication for a specific contact	Write	instance*		
				connect:InstanceId	
UpdateParticipantRoleConfig	Grants permission to update participant role configurations associated with a contact	Write	contact*		
			instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdatePhoneNumber	Grants permission to update phone number resources in an Amazon Connect instance or traffic distribution group	Write	instance*		
			phone-number*		
			traffic-distribution-group*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdatePhoneNumberMetadata	Grants permission to update the metadata of a phone number resource in an Amazon Connect instance or traffic distribution group	Write	phone-number*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePredefinedAttribute	Grants permission to update a predefined attribute in an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
UpdatePrompt	Grants permission to update a prompt's name, description, and Amazon S3 URI in an Amazon Connect instance	Write	prompt*		kms:Decrypt s3:GetObject s3:GetObjectAcl
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueHoursOfOperation	Grants permission to update queue hours of operation in an Amazon Connect instance	Write	hours-of-operation*		
			queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueMaxContacts	Grants permission to update queue capacity in an Amazon Connect instance	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueName	Grants permission to update a queue name and description in an Amazon Connect instance	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueOutboundCallerConfig	Grants permission to update queue outbound caller config in an Amazon Connect instance	Write	queue*		
			contact-flow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			phone-number		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueOutboundEmailConfig	Grants permission to update the outbound email configuration for a queue in an Amazon Connect instance	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQueueStatus	Grants permission to update queue status in an Amazon Connect instance	Write	queue*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateQuickConnectConfig	Grants permission to update the configuration of a quick connect in an Amazon Connect instance	Write	quick-connect*		
			contact-flow		
			queue		
			user		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateQuickConnectName	Grants permission to update a quick connect name and description in an Amazon Connect instance	Write	quick-connect*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRoutingProfileAgentAvailabilityTimer	Grants permission to update a routing profile agent availability timer in an Amazon Connect instance	Write	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileConcurrency	Grants permission to update the concurrency in a routing profile in an Amazon Connect instance	Write	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileDefaultOutboundQueue	Grants permission to update the outbound queue in a routing profile in an Amazon Connect instance	Write	queue*		
			routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRoutingProfileName	Grants permission to update a routing profile name and description in an Amazon Connect instance	Write	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRoutingProfileQueues	Grants permission to update the queues in routing profile in an Amazon Connect instance	Write	routing-profile*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateRule	Grants permission to update a rule for an existing Amazon Connect instance	Write	rule*		
				connect:InstanceId	
UpdateSecurityProfile	Grants permission to update a security profile group for a user in an Amazon Connect instance	Write	security-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateTaskTemplate	Grants permission to update task template belonging to a Amazon Connect instance	Write	task-template*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateTrafficDistribution	Grants permission to update traffic distribution for a traffic distribution group	Write	traffic-distribution-group*		
				aws:ResourceTag/${TagKey}	
UpdateUserHierarchy	Grants permission to update a hierarchy group for a user in an Amazon Connect instance	Write	user*		
			hierarchy-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserHierarchyGroupName	Grants permission to update a user hierarchy group name in an Amazon Connect instance	Write	hierarchy-group*		
				connect:InstanceId	
UpdateUserHierarchyStructure	Grants permission to update user hierarchy structure in an Amazon Connect instance	Write	instance*		
				connect:InstanceId	
UpdateUserIdentityInfo	Grants permission to update identity information for a user in an Amazon Connect instance	Write	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUserNotificationStatus	Grants permission to update the status of a user notification in an Amazon Connect instance	Write	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserPhoneConfig	Grants permission to update phone configuration settings for a user in an Amazon Connect instance	Write	user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserProficiencies	Grants permission to update user proficiencies from a user in an Amazon Connect instance	Write	instance*		
			user*		
				connect:InstanceId	
UpdateUserRoutingProfile	Grants permission to update a routing profile for a user in an Amazon Connect instance	Write	routing-profile*		
			user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateUserSecurityProfiles	Grants permission to update security profiles for a user in an Amazon Connect instance	Write	security-profile* user*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateViewContent	Grants permission to update a view's content in an Amazon Connect instance	Write	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateViewMetadata	Grants permission to update a view's metadata in an Amazon Connect instance	Write	customer-managed-view*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateWorkspaceMetadata	Grants permission to update workspace metadata in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateWorkspacePage	Grants permission to update a workspace page in an Amazon Connect instance	Write	workspace*		
			aws-managed-view		
			customer-managed-view		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateWorkspaceTheme	Grants permission to update workspace theme in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	
UpdateWorkspaceVisibility	Grants permission to update workspace visibility in an Amazon Connect instance	Write	workspace*		
				aws:ResourceTag/${TagKey} connect:InstanceId	

Resource types defined by Amazon 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:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey}
contact	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact/${ContactId}`	
user	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent/${UserId}`	aws:ResourceTag/${TagKey}
routing-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/routing-profile/${RoutingProfileId}`	aws:ResourceTag/${TagKey}
security-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/security-profile/${SecurityProfileId}`	aws:ResourceTag/${TagKey}
authentication-profile	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/authentication-profile/${AuthenticationProfileId}`	
hierarchy-group	`arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-group/${HierarchyGroupId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
data-table	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/data-table/${DataTableId}	aws:ResourceTag/${TagKey}
queue	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/queue/${QueueId}	aws:ResourceTag/${TagKey}
wildcard-queue	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/queue/*	
quick-connect	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/transfer-destination/${QuickConnectId}	aws:ResourceTag/${TagKey}
wildcard-quick-connect	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/transfer-destination/*	
contact-flow	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-flow/${ContactFlowId}	aws:ResourceTag/${TagKey}
task-template	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/task-template/${TaskTemplateId}	aws:ResourceTag/${TagKey}
contact-flow-module	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/flow-module/${ContactFlowModuleId}	aws:ResourceTag/${TagKey}
wildcard-contact-flow	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-flow/*	

Resource types	ARN	Condition keys
hours-of-operation	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/operating-hours/${HoursOfOperationId}	aws:ResourceTag/${TagKey}
agent-status	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-state/${AgentStatusId}	aws:ResourceTag/${TagKey}
wildcard-agent-status	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/agent-state/*	
legacy-phone-number	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/phone-number/${PhoneNumberId}	
wildcard-legacy-phone-number	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/phone-number/*	
phone-number	arn:${Partition}:connect:${Region}:${Account}:phone-number/${PhoneNumberId}	aws:ResourceTag/${TagKey}
wildcard-phone-number	arn:${Partition}:connect:${Region}:${Account}:phone-number/*	aws:ResourceTag/${TagKey}
integration-association	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/integration-association/${IntegrationAssociationId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
use-case	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/use-case/${UseCaseId}	aws:ResourceTag/${TagKey}
vocabulary	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/vocabulary/${VocabularyId}	aws:ResourceTag/${TagKey}
traffic-distribution-group	arn:${Partition}:connect:${Region}:${Account}:traffic-distribution-group/${TrafficDistributionGroupId}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/rule/${RuleId}	aws:ResourceTag/${TagKey}
evaluation-form	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/evaluation-form/${FormId}	aws:ResourceTag/${TagKey}
contact-evaluation	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/contact-evaluation/${EvaluationId}	aws:ResourceTag/${TagKey}
prompt	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/prompt/${PromptId}	aws:ResourceTag/${TagKey}
customer-managed-view	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/view/${ViewId}	aws:ResourceTag/${TagKey}
aws-managed-view	arn:${Partition}:connect:${Region}:aws:view/${ViewId}	

Resource types	ARN	Condition keys
qualified-customer-managed-view	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/view/${ViewId}:${ViewQualifier}	aws:ResourceTag/${TagKey}
qualified-aws-managed-view	arn:${Partition}:connect:${Region}:aws:view/${ViewId}:${ViewQualifier}	
customer-managed-view-version	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/view/${ViewId}:${ViewVersion}	aws:ResourceTag/${TagKey}
attached-file	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/file/${FileId}	aws:ResourceTag/${TagKey}
email-address	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/email-address/${EmailAddressId}	aws:ResourceTag/${TagKey}
ai-agent	arn:${Partition}:wisdom:${Region}:${Account}:ai-agent/${AssistantId}/${AIAgentId}:${Version}	
workspace	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
notification	arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}/notification/${NotificationId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Connect

Amazon 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by using tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by using tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by using tag keys in the request	ArrayOfString
connect:AssignmentType	Filters access by restricting access to create contacts based on Assignment Type	String
connect:AttributeType	Filters access by the attribute type of the Amazon Connect instance	String
connect:Channel	Filters access by Channel	String
connect:ContactAssociationId	Filters access by ContactAssociationId	String
connect:ContactInitiationMethod	Filters access by restricting access to create contacts based on the initiation method of the contact	String
connect:ExpressionValue	Filters access by restricting data table operations based on expression type	String

Condition keys	Description	Type
connect:FlowType	Filters access by Flow type	ArrayOfString
connect:InstanceId	Filters access by restricting federation into specified Amazon Connect instances	String
connect:ListRealtimeContactAnalysisSegmentsByOutputType	Filters access by restricting the listed segments using the output type of the Amazon Connect Contact Lens real-time segment	String
connect:ListRealtimeContactAnalysisSegmentsBySegmentType	Filters access by restricting the listed segments using the segment types of the Amazon Connect Contact Lens real-time segment	ArrayOfString
connect:MonitorCapabilities	Filters access by restricting the monitor capabilities of the user in the request	ArrayOfString
connect:PreferredUserArn	Filters access by PreferredUserArn	ARN
connect:PrimaryAttribute/${PrimaryAttribute}	Filters access by restricting which primary attributes the user can manage	String
connect:SearchContactsByContactAnalysis	Filters access by restricting searches using analysis outputs from Amazon Connect Contact Lens	ArrayOfString

Condition keys	Description	Type
connect:SearchTag/${TagKey}	Filters access by TagFilter condition passed in the search request	String
connect:StorageResourceType	Filters access by restricting the storage resource type of the Amazon Connect instance storage configuration	String
connect:Subtype	Filters access by restricting creation of a contact for specific subtypes	String
connect:UserArn	Filters access by UserArn	ARN

Actions, resources, and condition keys for Amazon Connect Cases

Amazon Connect Cases (service prefix: `cases`) 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 Connect Cases
- Resource types defined by Amazon Connect Cases
- Condition keys for Amazon Connect Cases

Actions defined by Amazon Connect Cases

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetCaseRule	Grants permission to retrieve information about the case rules in the case domain	Read	CaseRule*		
			Domain*		
BatchGetField	Grants permission to retrieve information about the fields in the case domain	Read	Domain*		
			Field*		
BatchPutFieldOptions	Grants permission to update the field options in the case domain	Write	Domain*		
			Field*		
CreateCase	Grants permission to create a case in the case domain	Write	Case*		
			Domain*		
			Field*		
			Template*		
				connect:UserArn	
CreateCaseRule	Grants permission to create a case rule in the case domain	Write	CaseRule*		
			Domain*		
CreateDomain	Grants permission to create a new case domain	Write			
CreateField	Grants permission to create a field in the case domain	Write	Domain*		
			Field*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLayout	Grants permission to create a layout in the case domain	Write	Domain*		
			Layout*		
CreateRelatedItem	Grants permission to create a related item associated to a case in the case domain	Write	Case*		
			Domain*		
			RelatedItem*		
				connect:UserArn	
CreateTemplate	Grants permission to create a template in the case domain	Write	Domain*		
			Layout*		
			Template*		
DeleteCase	Grants permission to delete the case in the case domain	Write	Case*		
			Domain*		
DeleteCaseRule	Grants permission to delete the case rule in the case domain	Write	CaseRule*		
			Domain*		
DeleteDomain	Grants permission to delete the domain	Write	Domain*		
DeleteField	Grants permission to delete the field in the case domain	Write	Domain*		
			Field*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLayout	Grants permission to delete the layout in the case domain	Write	Domain*		
			Layout*		
DeleteRelatedItem	Grants permission to delete the related item associated to the case in the case domain	Write	Case*		
			Domain*		
			RelatedItem*		
DeleteTemplate	Grants permission to delete the template in the case domain	Write	Domain*		
			Template*		
GetCase	Grants permission to retrieve information about a case in the case domain	Read	Case*		
			Domain*		
			Field*		
GetCaseAuditEvents	Grants permission to view audit history of a case	Read	Case*		
			Domain*		
GetCaseEventConfiguration	Grants permission to retrieve information about the case event configuraton in the case domain	Read	Domain*		
GetDomain	Grants permission to retrieve information about the case domain	Read	Domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLayout	Grants permission to retrieve information about the layout in the case domain	Read	Domain*		
			Layout*		
GetTemplate	Grants permission to retrieve information about the template in the case domain	Read	Domain*		
			Template*		
ListCaseRules	Grants permission to list case rules in the case domain	List	Domain*		
ListCasesForContact	Grants permission to list cases for a specific contact in the case domain	List	Domain*		
ListDomains	Grants permission to list all domains in the aws account	List			
ListFieldOptions	Grants permission to list field options for a single select field in the case domain	List	Domain*		
			Field*		
ListFields	Grants permission to list fields in the case domain	List	Domain*		
ListLayouts	Grants permission to list layouts in the case domain	List	Domain*		
ListTagsForResource	Grants permission to list the tags for the specified resource	Read			
ListTemplates	Grants permission to list templates in the case domain	List	Domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutCaseEventConfiguration	Grants permission to insert or update the case event configuration in the case domain	Write	Domain*		
SearchCases	Grants permission to search for cases in the case domain	Read	Domain*		
SearchRelatedItems	Grants permission to search for related items associated to the case in the case domain	Read	Case*		
			Domain*		
TagResource	Grants permission to add the specified tags to the specified resource	Tagging	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	Case		
			CaseRule		
			Domain		
			Field		
			Layout		
			RelatedItem		
			Template		
				aws:TagKeys	
UpdateCase	Grants permission to update the field values on the case in the case domain	Write	Case*		
			Domain*		
			Field*		
				connect:UserArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCaseRule	Grants permission to update the case rule in the case domain	Write	CaseRule*		
			Domain*		
UpdateField	Grants permission to update the field in the case domain	Write	Domain*		
			Field*		
UpdateLayout	Grants permission to update the layout in the case domain	Write	Domain*		
			Layout*		
UpdateTemplate	Grants permission to update the template in the case domain	Write	Domain*		
			Template*		

Resource types defined by Amazon Connect Cases

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
Case	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}`	aws:ResourceTag/${TagKey}
Domain	`arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Field	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/field/${FieldId}	aws:ResourceTag/${TagKey}
Layout	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/layout/${LayoutId}	aws:ResourceTag/${TagKey}
RelatedItem	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case/${CaseId}/related-item/${RelatedItemId}	aws:ResourceTag/${TagKey}
Template	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/template/${TemplateId}	aws:ResourceTag/${TagKey}
CaseRule	arn:${Partition}:cases:${Region}:${Account}:domain/${DomainId}/case-rule/${CaseRuleId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Connect Cases

Amazon Connect Cases defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString
connect:UserArn	Filters access by connect's UserArn	ARN

Actions, resources, and condition keys for Amazon Connect Customer Profiles

Amazon Connect Customer Profiles (service prefix: `profile`) 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 Connect Customer Profiles
- Resource types defined by Amazon Connect Customer Profiles
- Condition keys for Amazon Connect Customer Profiles

Actions defined by Amazon Connect Customer 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddProfileKey	Grants permission to add a profile key	Write	domains*		
BatchGetCalculatedAttributeForProfile	Grants permission to retrieve a calculated attribute for the specific profiles in the domain	Read	calculated-attributes*		
			domains*		
BatchGetProfile	Grants permission to get profiles in the domain	Read	domains*		
CreateCalculatedAttributeDefinition	Grants permission to create a calculated attribute definition in the domain	Write	calculated-attributes*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		
CreateDomain	Grants permission to create a Domain	Write	domains*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateDomainLayout	Grants permission to create a layout in the domain	Write	domains*		
			layouts*	aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateEventStream	Grants permission to put an event stream in a domain	Write	domains*		iam:PutRolePolicy kinesis:DescribeStreamSummary
			event-streams*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventTrigger	Grants permission to create an event trigger in the domain	Write	domains*		
			event-triggers*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationWorkflow	Grants permission to create an integration workflow in a domain	Write	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Grants permission to create a profile in the domain	Write	domains*		
CreateRecommender	Grants permission to create a Recommender in the domain	Write	domains*		
			recommenders*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentDefinition	Grants permission to create a segment definition in the domain	Write	domains*		
			segment-definitions*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSegmentEstimate	Grants permission to create a segment estimate in the domain	Write	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSegmentSnapshot	Grants permission to create a segment snapshot in the domain	Write	domains*		
			segment-definitions*		
CreateSnapshot [permission only]	Grants permission to create a snapshot in the domain	Write	domains*		
CreateUploadJob	Grants permission to create an upload job in the domain	Write	domains*		
DeleteCalculatedAttributeDefinition	Grants permission to delete a calculated attribute definition in the domain	Write	calculated-attributes*		
			domains*		
DeleteDomain	Grants permission to delete a Domain	Write	domains*		
DeleteDomainLayout	Grants permission to delete a layout in the domain	Write	domains*		
			layouts*		
DeleteDomainObjectType	Grants permission to delete a specific domain object type in the domain	Write	domain-object-types*		
			domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEventStream	Grants permission to delete an event stream in a domain	Write	domains*		iam:DeleteRolePolicy
			event-streams*		
DeleteEventTrigger	Grants permission to delete an event trigger in the domain	Write	domains*		
			event-triggers*		
DeleteIntegration	Grants permission to delete a integration in a domain	Write	domains*		
			integrations*		
DeleteProfile	Grants permission to delete a profile	Write	domains*		
DeleteProfileKey	Grants permission to delete a profile key	Write	domains*		
DeleteProfileObject	Grants permission to delete a profile object	Write	domains*		
			object-types*		
DeleteProfileObjectType	Grants permission to delete a specific profile object type in the domain	Write	domains*		
			object-types*		
DeleteRecommender	Grants permission to delete a recommender in a domain	Write	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			recommenders*		
DeleteSegmentDefinition	Grants permission to delete a segment definition in the domain	Write	domains*		
			segment-definitions*		
DeleteWorkflow	Grants permission to delete a workflow in a domain	Write	domains*		
DetectProfileObjectType	Grants permission to auto detect object type	Read	domains*		
GetAutoMergingPreview	Grants permission to get a preview of auto merging in a domain	Read	domains*		
GetCalculatedAttributeDefinition	Grants permission to get a calculated attribute definition in the domain	Read	calculated-attributes*		
			domains*		
GetCalculatedAttributeForProfile	Grants permission to retrieve a calculated attribute for a specific profile in the domain	Read	calculated-attributes*		
			domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDomain	Grants permission to get a specific domain in an account	Read	domains*		
GetDomainLayout	Grants permission to get a layout in the domain	Read	domains*		
			layouts*		
GetDomainObjectType	Grants permission to get a specific domain object type in the domain	Read	domain-object-types*		
			domains*		
GetEventStream	Grants permission to get a specific event stream in a domain	Read	domains*		kinesis:DescribeStreamSummary
			event-streams*		
GetEventTrigger	Grants permission to get an event trigger in the domain	Read	domains*		
			event-triggers*		
GetIdentityResolutionJob	Grants permission to get an identity resolution job in a domain	Read	domains*		
GetIntegration	Grants permission to get a specific integrations in a domain	Read	domains*		
			integrations*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMatches	Grants permission to get profile matches in a domain	List	domains*		
GetObjectTypeAttributeStatistics	Grants permission to get statistics of a specific attribute for object type in the domain	Read	domains*		
			object-types*		
GetProfileHistoryRecord	Grants permission to get a profile history record for a profile in a domain	Read	domains*		
GetProfileInsights	Grants permission to list insights for a profile	Read	domains*		
GetProfileObjectType	Grants permission to get a specific profile object type in the domain	Read	domains*		
			object-types*		
GetProfileObjectTypeTemplate	Grants permission to get a specific object type template	Read			
GetProfileRecommendations	Grants permission to list recommendations for a profile	Read	domains*		
			recommenders*		
GetRecommender	Grants permission to get Recommender details in a domain	Read	domains*		
			recommenders*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSegmentDefinition	Grants permission to get a segment definition in the domain	Read	domains*		
			segment-definitions*		
GetSegmentEstimate	Grants permission to get a segment estimate in the domain	Read	domains*		
GetSegmentMembership	Grants permission to determine if the given profiles are part of a segment in the domain	Read	domains*		
			segment-definitions*		
GetSegmentSnapshot	Grants permission to get a segment snapshot in the domain	Read	domains*		
			segment-definitions*		
GetSimilarProfiles	Grants permission to get all the similar profiles in the domain	List	domains*		
GetSnapshot [permission only]	Grants permission to get a snapshot in the domain	Read	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUploadJob	Grants permission to get details of an upload job in the domain	Read	domains*		
GetUploadJobPath	Grants permission to get a pre-signed URL to upload file for an upload job	Read	domains*		
GetWorkflow	Grants permission to get workflow details in a domain	Read	domains*		
GetWorkflowSteps	Grants permission to get workflow step details in a domain	Read	domains*		
ListAccountIntegrations	Grants permission to list all the integrations in the account	List			
ListCalculatedAttributeDefinitions	Grants permission to list all the calculated attribute definitions in the domain	List	domains*		
ListCalculatedAttributesForProfile	Grants permission to list all calculated attributes for a specific profile in the domain	List	domains*		
ListDomainLayouts	Grants permission to list all the layouts in the domain	List	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDomainObjectTypes	Grants permission to list all the domain object types in the domain	List	domains*		
ListDomainObjects	Grants permission to list domain objects in a domain	List	domain-object-types*		
			domains*		
ListDomains	Grants permission to list all the domains in an account	List			
ListEventStreams	Grants permission to list all the event streams in a specific domain	List	domains*		
ListEventTriggers	Grants permission to list all the event triggers in the domain	List	domains*		
ListIdentityResolutionJobs	Grants permission to list identity resolution jobs in a domain	List	domains*		
ListIntegrations	Grants permission to list all the integrations in a specific domain	List	domains*		
ListObjectTypeAttributeValues	Grants permission to list values of a specific attribute for object type in the domain	List	domains*		
			object-types*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListObjectTypeAttributes	Grants permission to list all the attributes of a specific object type in the domain	List	domains*		
			object-types*		
ListProfileAttributeValues	Grants permission to list all the values of a profile attribute in the domain	List	domains*		
ListProfileHistoryRecords	Grants permission to list all the profile history records for a profile in a domain	List	domains*		
ListProfileObjectTypeTemplates	Grants permission to list all the profile object type templates in the account	List			
ListProfileObjectTypes	Grants permission to list all the profile object types in the domain	List	domains*		
ListProfileObjects	Grants permission to list all the profile objects for a profile	List	domains*		
			object-types*		
ListRecommenderRecipes	Grants permission to list all the Recommenders Recipes in the domain	List			
ListRecommenders	Grants permission to list all the Recommenders in the domain	List	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRuleBasedMatches	Grants permission to list all the rule-based matching result in the domain	List	domains*		
ListSegmentDefinitions	Grants permission to list all the segment definitions in the domain	List	domains*		
ListTagsForResource	Grants permission to list tags for a resource	Read	calculated-attributes		
			domain-object-types		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			recommenders		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			segment-definitions		
ListUploadJobs	Grants permission to list all upload jobs in the domain	List	domains*		
ListWorkflows	Grants permission to list all the workflows in a specific domain	List	domains*		
MergeProfiles	Grants permission to merge profiles in a domain	Write	domains*		
PutDomainObjectType	Grants permission to put a specific domain object type in the domain	Write	domain-object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
			domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutIntegration	Grants permission to put a integration in a domain	Write	domains*		app-integrations:CreateDataIntegrationAssociation app-integrations:DeleteDataIntegrationAssociation app-integrations:GetDataIntegration app-integrations:ListDataIntegrationAssociations kms:CreateGrant

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integrations*	aws:RequestTag/${TagKey} aws:TagKeys	
PutProfileObject	Grants permission to put an object for a profile	Write	domains*		
			object-types*		
PutProfileObjectType	Grants permission to put a specific profile object type in the domain	Write	domains*		
			object-types*	aws:RequestTag/${TagKey} aws:TagKeys	
SearchProfiles	Grants permission to search for profiles in a domain	Read	domains*		
StartRecommender	Grants permission to start a recommender in a domain	Write	domains*		
			recommenders*		
StartUploadJob	Grants permission to start an upload job in the domain	Write	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopRecommender	Grants permission to stop a recommender in a domain	Write	domains*		
			recommenders*		
StopUploadJob	Grants permission to stop an upload job in the domain	Write	domains*		
TagResource	Grants permission to adds tags to a resource	Tagging	calculated-attributes		
			domain-object-types		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		
			object-types		
			recommenders		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			segment-definitions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	calculated-attributes		
			domain-object-types		
			domains		
			event-streams		
			event-triggers		
			integrations		
			layouts		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			object-types		
			recommenders		
			segment-definitions		
				aws:TagKeys	
UpdateCalculatedAttributeDefinition	Grants permission to update a calculated attribute definition in the domain	Write	calculated-attributes*		
			domains*		
UpdateDomain	Grants permission to update a Domain	Write	domains*		iam:CreateServiceLinkedRole
UpdateDomainLayout	Grants permission to update a layout in the domain	Write	domains*		
			layouts*		
UpdateEventTrigger	Grants permission to update an event trigger in the domain	Write	domains*		
			event-triggers*		
UpdateProfile	Grants permission to update a profile in the domain	Write	domains*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRecommender	Grants permission to update a Recommender in the domain	Write	domains*		
			recommenders*		

Resource types defined by Amazon Connect Customer 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
domains	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}`	aws:ResourceTag/${TagKey}
object-types	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/object-types/${ObjectTypeName}`	aws:ResourceTag/${TagKey}
integrations	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/integrations/${Uri}`	aws:ResourceTag/${TagKey}
event-streams	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-streams/${EventStreamName}`	aws:ResourceTag/${TagKey}
calculated-attributes	`arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/calc`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
	ulated-attributes/${CalculatedAttribuuteName}	
segment-definitions	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/segment-definitions/${SegmentDefinitionName}	aws:ResourceTag/${TagKey}
event-triggers	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/event-triggers/${EventTriggerName}	aws:ResourceTag/${TagKey}
layouts	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/layouts/${LayoutDefinitionName}	aws:ResourceTag/${TagKey}
recommenders	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/recommenders/${RecommenderTypeName}	aws:ResourceTag/${TagKey}
domain-object-types	arn:${Partition}:profile:${Region}:${Account}:domains/${DomainName}/domain-object-types/${ObjectTypeName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Connect Customer Profiles

Amazon Connect Customer 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the customer profile service	String
aws:ResourceTag/${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 customer profile service	ArrayOfString

Actions, resources, and condition keys for Amazon Connect Health

Amazon Connect Health (service prefix: `health-agent`) 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 Connect Health
- Resource types defined by Amazon Connect Health
- Condition keys for Amazon Connect Health

Actions defined by Amazon Connect Health

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateSubscription	Grants permission to activate a subscription to enable billing for a user	Write	Domain*		
			Subscription*		
CancelAppointment [permission only]	Grants permission to cancel an appointment	Write	Domain*		
			Integration*		
CreateAgent [permission only]	Grants permission to create a new agent with an initial version in DRAFT state	Write	Agent*		
			Domain*		
CreateDomain	Grants permission to create a new domain for managing HealthAgent resources	Write		aws:RequestTag/${TagKey}	health-agent:TagResource
				aws:TagKeys	iam:PassRole
CreateIntegration [permission only]	Grants permission to create a new integration for a domain	Write	Domain*		
			Integration*		
CreateSession [permission only]	Grants permission to create a new session with specified agent configurations	Write	Agent*		
			Domain*		
			Session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubscription	Grants permission to create a new subscription within a domain for billing and user management	Write	Domain*		
			Subscription*		
DeactivateSubscription	Grants permission to deactivate a subscription to stop billing for a user	Write	Domain*		
			Subscription*		
DeleteAgent [permission only]	Grants permission to delete an agent configuration and all its versions	Write	Agent*		
			Domain*		
DeleteDomain	Grants permission to delete a domain and all associated resources	Write	Domain*		
DeleteIntegration [permission only]	Grants permission to delete an integration	Write	Domain*		
			Integration*		
GetAgent [permission only]	Grants permission to retrieve an agent configuration, defaulting to the most recent version if not specified	Read	Agent*		
			Domain*		
GetCareTeamProvider [permission only]	Grants permission to retrieve the care team provider of a patient	Read	Domain*		
			Integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDomain	Grants permission to retrieve information about a domain	Read	Domain*		
GetIntegration [permission only]	Grants permission to get an existing integration	Read	Domain*		
			Integration*		
GetMedicalScribeListeningSession	Grants permission to retrieve details about an existing Medical Scribe listening session	Read	Domain*		
			Subscription*		
GetPatient [permission only]	Grants permission to retrieve patient information	Read	Domain*		
			Integration*		
GetPatientInsightsJob	Grants permission to get details of a started patient insights job	Read	Domain*		
			PatientInsightsJob*		
GetPractitioner [permission only]	Grants permission to retrieve practitioner information	Read	Domain*		
			Integration*		
GetSessionContext [permission only]	Grants permission to retrieve structured session context including attributes and collected data	Read	Domain*		
			Session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSubscription	Grants permission to retrieve information about a subscription	Read	Domain*		
			Subscription*		
InvokeAgent [permission only]	Grants permission to invoke an agent within a session with streaming response support	Write	Domain*		
			Session*		
ListAgents [permission only]	Grants permission to list all agents in a domain	List	Domain*		
ListAppointmentSlots [permission only]	Grants permission to list available appointment slots	Read	Domain*		
			Integration*		
ListDomains	Grants permission to list domains for a given account	List			
ListIntegrations [permission only]	Grants permission to list integrations for a domain	List	Domain*		
ListPatientAppointments [permission only]	Grants permission to list patient appointments	Read	Domain*		
			Integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPatientInsuranceCoverages [permission only]	Grants permission to list patient insurance coverages	Read	Domain*		
			Integration*		
ListProviders [permission only]	Grants permission to retrieve active providers available for scheduling appointments with a patient	Read	Domain*		
			Integration*		
ListSubscriptions	Grants permission to list all subscriptions within a domain	List	Domain*		
ListTagsForResource	Grants permission to list the tags for the specified resource	List	Domain		
MatchPatient [permission only]	Grants permission to match a patient	Read	Domain*		
			Integration*		
PublishAgent [permission only]	Grants permission to publish an agent configuration version	Write	Agent*		
			Domain*		
RescheduleAppointment [permission only]	Grants permission to reschedule an appointment	Write	Domain*		
			Integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ScheduleAppointment [permission only]	Grants permission to schedule an appointment for a patient	Write	Domain*		
			Integration*		
StartMedicalScribeListeningSession	Grants permission to start a new Medical Scribe listening session for real-time audio transcription	Write	Domain*		
			Subscription*		
StartPatientInsightsJob	Grants permission to start a new patient insights job	Write	Domain*		
			PatientInsightsJob*		
TagResource	Grants permission to add the specified tags to the specified resource	Tagging	Domain	aws:ResourceTag/${TagKey}	
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove the tags identified by the TagKeys list from a resource	Tagging	Domain		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgent [permission only]	Grants permission to update a draft agent configuration, creating a new draft version if none exists	Write	Agent*		
			Domain*		
UpdateIntegration [permission only]	Grants permission to update an existing integration	Write	Domain*		
			Integration*		
UpdateSession [permission only]	Grants permission to update session attributes such as departmentId and appointmentType	Write	Domain*		
			Session*		

Resource types defined by Amazon Connect Health

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:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}
PatientInsightsJob	`arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/patient-insights-job/${JobId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Subscription	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/subscription/${SubscriptionId}	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/integration/${IntegrationId}	aws:ResourceTag/${TagKey}
Agent	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/agent/${AgentId}	aws:ResourceTag/${TagKey}
Session	arn:${Partition}:health-agent:${Region}:${Account}:domain/${DomainId}/session/${SessionId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Connect Health

Amazon Connect Health defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Connect Outbound Campaigns

Amazon Connect Outbound Campaigns (service prefix: `connect-campaigns`) 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 Connect Outbound Campaigns

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCampaign	Grants permission to create a campaign	Write	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteCampaign	Grants permission to delete a campaign	Write	campaign*		
DeleteCampaignChannelSubtypeConfig	Grants permission to delete the channel subtype configuration of a campaign	Write	campaign*		
DeleteCampaignCommunicationLimits	Grants permission to delete the communication limits configuration of a campaign	Write	campaign*		
DeleteCampaignCommunicationTime	Grants permission to delete the communication time configuration of a campaign	Write	campaign*		
DeleteConnectInstanceConfig	Grants permission to remove configuration information for an Amazon Connect instance	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConnectInstanceIntegration	Grants permission to remove integration information for an Amazon Connect instance	Write			
DeleteInstanceOnboardingJob	Grants permission to remove onboarding job for an Amazon Connect instance	Write			
DescribeCampaign	Grants permission to describe a specific campaign	Read	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignState	Grants permission to get state of a campaign	Read	campaign*		
				aws:RequestTag/${TagKey}	
GetCampaignStateBatch	Grants permission to get state of campaigns	Read	campaign*		
				aws:RequestTag/${TagKey}	
GetConnectInstanceConfig	Grants permission to get configuration information for an Amazon Connect instance	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceCommunicationLimits	Grants permission to get the communication limits configuration of an Amazon Connect instance	Read			
GetInstanceOnboardingJobStatus	Grants permission to get onboarding job status for an Amazon Connect instance	Read			
ListCampaigns	Grants permission to provide summary of all campaigns	List		aws:RequestTag/${TagKey}	
ListConnectInstanceIntegrations	Grants permission to provide summary of all integrations with an Amazon Connect instance	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	campaign		
				aws:ResourceTag/${TagKey}	
PauseCampaign	Grants permission to pause a campaign	Write	campaign*		
PutConnectInstanceIntegration	Grants permission to put an integration configuration with an Amazon Connect instance	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDialRequestBatch	Grants permission to create dial requests for the specified campaign	Write	campaign*		
PutInstanceCommunicationLimits	Grants permission to put the communication limits configuration of an Amazon Connect instance	Write			
PutOutboundRequestBatch	Grants permission to create dial requests for the specified campaign	Write	campaign*		
PutProfileOutboundRequestBatch	Grants permission to create profile outbound requests for the specified campaign	Write	campaign*		
ResumeCampaign	Grants permission to resume a campaign	Write	campaign*		
StartCampaign	Grants permission to start a campaign	Write	campaign*		
StartInstanceOnboardingJob	Grants permission to start onboarding job for an Amazon Connect instance	Write			
StopCampaign	Grants permission to stop a campaign	Write	campaign*		
TagResource	Grants permission to tag a resource	Tagging	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	campaign*		
				aws:TagKeys	
UpdateCampaignChannelSubtypeConfig	Grants permission to update the channel subtype configuration of a campaign	Write	campaign*		
UpdateCampaignCommunicationLimits	Grants permission to update the communication limits configuration of a campaign	Write	campaign*		
UpdateCampaignCommunicationTime	Grants permission to update the communication time configuration of a campaign	Write	campaign*		
UpdateCampaignDialerConfig	Grants permission to update the dialer configuration of a campaign	Write	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCampaignFlowAssociation	Grants permission to update the flow association of a campaign	Write	campaign*		
UpdateCampaignName	Grants permission to update the name of a campaign	Write	campaign*		
UpdateCampaignOutboundCallConfig	Grants permission to update the outbound call configuration of a campaign	Write	campaign*		
UpdateCampaignSchedule	Grants permission to update the schedule of a campaign	Write	campaign*		
UpdateCampaignSource	Grants permission to update the source of a campaign	Write	campaign*		

Resource types defined by Amazon Connect Outbound Campaigns

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
campaign	arn:${Partition}:connect-campaigns:${Region}:${Account}:campaign/${CampaignId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Connect Outbound Campaigns

Amazon Connect Outbound Campaigns defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Connect Voice ID

Amazon Connect Voice ID (service prefix: voiceid) 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 Connect Voice ID

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFraudster	Grants permission to associate a fraudster with a watchlist	Write	domain*		
CreateDomain	Grants permission to create a domain	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWatchlist	Grants permission to create a watchlist	Write	domain*		
DeleteDomain	Grants permission to delete a domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFraudster	Grants permission to delete a fraudster	Write	domain*		
DeleteSpeaker	Grants permission to delete a speaker	Write	domain*		
DeleteWatchlist	Grants permission to delete a watchlist	Write	domain*		
DescribeComplianceConsent [permission only]	Grants permission to describe compliance consent	Read			
DescribeDomain	Grants permission to describe a domain	Read	domain*		
DescribeFraudster	Grants permission to describe a fraudster	Read	domain*		
DescribeFraudsterRegistrationJob	Grants permission to describe a fraudster registration job	Read	domain*		
DescribeSpeaker	Grants permission to describe a speaker	Read	domain*		
DescribeSpeakerEnrollmentJob	Grants permission to describe a speaker enrollment job	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWatchlist	Grants permission to describe a watchlist	Read	domain*		
DisassociateFraudster	Grants permission to disassociate a fraudster from a watchlist	Write	domain*		
EvaluateSession	Grants permission to evaluate a session	Write	domain*		
ListDomains	Grants permission to list domains for an account	List			
ListFraudsterRegistrationJobs	Grants permission to list fraudster registration jobs for a domain	List	domain*		
ListFraudsters	Grants permission to list fraudsters for a domain or watchlist	List	domain*		
ListSpeakerEnrollmentJobs	Grants permission to list speaker enrollment jobs for a domain	List	domain*		
ListSpeakers	Grants permission to list speakers for a domain	List	domain*		
ListTagsForResource	Grants permission to list tags for a Voice ID resource	Read	domain		
ListWatchlists	Grants permission to list watchlists for a domain	List	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
OptOutSpeaker	Grants permission to opt out a speaker	Write	domain*		
RegisterComplianceConsent [permission only]	Grants permission to register compliance consent	Write			
StartFraudsterRegistrationJob	Grants permission to start a fraudster registration job	Write	domain*		
StartSpeakerEnrollmentJob	Grants permission to start a speaker enrollment job	Write	domain*		
TagResource	Grants permission to tag a Voice ID resource	Tagging	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag from a Voice ID resource	Tagging	domain		
				aws:TagKeys	
UpdateDomain	Grants permission to update a domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWatchlist	Grants permission to update a watchlist	Write	domain*		

Resource types defined by Amazon Connect Voice ID

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:${Partition}:voiceid:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Connect Voice ID

Amazon Connect Voice ID defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Connector Service

AWS 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 AWS Connector Service
- Resource types defined by AWS Connector Service
- Condition keys for AWS Connector Service

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConnectorHealth [permission only]	Retrieves all health metrics that were published from the Server Migration Connector.	Read			
RegisterConnector [permission only]	Registers AWS Connector with AWS Connector Service.	Write			
ValidateConnectorId [permission only]	Validates Server Migration Connector Id that was registered with AWS Connector Service.	Read			

Resource types defined by AWS Connector Service

AWS Connector Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Connector Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Management Console Mobile App

AWS Management Console Mobile App (service prefix: `consoleapp`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Management Console Mobile App

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDeviceIdentity	Grants permission to retrieve the device identity for a Console Mobile App device	Read	DeviceIdentity*		
ListDeviceIdentities	Grants permission to retrieve a list of device identities	List			

Resource types defined by AWS Management Console Mobile App

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
DeviceIdentity	`arn:${Partition}:consoleapp::${Account}:device/${DeviceId}/identity/${IdentityId}`	

Condition keys for AWS Management Console Mobile App

Console Mobile App has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Consolidated Billing

AWS 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 AWS Consolidated Billing
- Resource types defined by AWS Consolidated Billing
- Condition keys for AWS Consolidated Billing

Actions defined by AWS 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 AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountBillingRole [permission only]	Grants permission to get account role (Payer, Linked, Regular)	Read			
ListLinkedAccounts [permission only]	Grants permission to get list of member/linked accounts	List			

Resource types defined by AWS Consolidated Billing

AWS Consolidated Billing does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Consolidated Billing, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Control Catalog

AWS Control Catalog (service prefix: `controlcatalog`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Control Catalog

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetControl	Grants permission to return details about a specific control	Read	control*		
ListCommonControls	Grants permission to return a paginated list of common controls from the AWS Control Catalog	List			
ListControlMappings	Grants permission to return a paginated list of control mappings from the AWS Control Catalog	List			
ListControls	Grants permission to return a paginated list of all available controls in the AWS Control Catalog library	List	control*		
ListDomains	Grants permission to return a paginated list of domains from the AWS Control Catalog	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListObjectives	Grants permission to return a paginated list of objectives from the AWS Control Catalog	List			

Resource types defined by AWS Control Catalog

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
common-control	`arn:${Partition}:controlcatalog:::common-control/${CommonControlId}`	
control	`arn:${Partition}:controlcatalog:::control/${ControlId}`	
domain	`arn:${Partition}:controlcatalog:::domain/${DomainId}`	
objective	`arn:${Partition}:controlcatalog:::objective/${ObjectiveId}`	

Condition keys for AWS Control Catalog

Control Catalog has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Control Tower

AWS Control Tower (service prefix: `controltower`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Control Tower
- Resource types defined by AWS Control Tower
- Condition keys for AWS Control Tower

Actions defined by AWS Control Tower

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLandingZone	Grants permission to create a landing zone	Write		aws:RequestTag/${TagKey}	controltower:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateManagedAccount [permission only]	Grants permission to create an account managed by AWS Control Tower	Write			
DeleteLandingZone	Grants permission to delete AWS Control Tower landing zone	Write	LandingZone*		
DeregisterManagedAccount [permission only]	Grants permission to deregister an account created through the account factory from AWS Control Tower	Write			
DeregisterOrganizationalUnit [permission only]	Grants permission to deregister an organizational unit from AWS Control Tower management	Write			
DescribeAccountFactoryConfig [permission only]	Grants permission to describe the current account factory configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCoreService [permission only]	Grants permission to describe resources managed by core accounts in AWS Control Tower	Read			
DescribeGuardrail [permission only]	Grants permission to describe a guardrail	Read			
DescribeGuardrailForTarget [permission only]	Grants permission to describe a guardrail for a organizational unit	Read			
DescribeLandingZoneConfiguration [permission only]	Grants permission to describe the current Landing Zone configuration	Read			
DescribeManagedAccount [permission only]	Grants permission to describe an account created through account factory	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeManagedOrganizationalUnit [permission only]	Grants permission to describe an AWS Organizations organizational unit managed by AWS Control Tower	Read			
DescribeRegisterOrganizationalUnitOperation [permission only]	Grants permission to describe a Register Organizational Unit Operation	Read			
DescribeSingleSignOn [permission only]	Grants permission to describe the current AWS Control Tower IAM Identity Center configuration	Read			
DisableBaseline	Grants permission to disable a Baseline on a target	Write	EnabledBaseline*		
DisableControl	Grants permission to remove a control from an organizational unit	Write	EnabledControl*		
DisableGuardrail [permission only]	Grants permission to disable a guardrail from an organizational unit	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableBaseline	Grants permission to enable a Baseline on a target	Write		aws:RequestTag/${TagKey} aws:TagKeys	controltower:TagResource
EnableControl	Grants permission to activate a control for an organizational unit	Write	EnabledControl		controltower:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableGuardrail [permission only]	Grants permission to enable a guardrail to an organizational unit	Write			
GetAccountInfo [permission only]	Grants permission to describe an account email and validate that it exists	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAvailableUpdates [permission only]	Grants permission to list available updates for the current AWS Control Tower deployment	Read			
GetBaseline	Grants permission to get Baseline details	Read	Baseline*		
GetBaselineOperation	Grants permission to get the current status of a particular Baseline operation	Read			
GetControlOperation	Grants permission to get the current status of a particular EnabledControl or DisableControl operation	Read			
GetEnabledBaseline	Grants permission to get an enabled Baseline	Read	EnabledBaseline*		
GetEnabledControl	Grants permission to get an enabled control from an organizational unit	Read	EnabledControl*		
GetGuardrailComplianceStatus [permission only]	Grants permission to get the current compliance status of a guardrail	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHomeRegion [permission only]	Grants permission to get the home region of the AWS Control Tower setup	Read			
GetLandingZone	Grants permission to get the current status of the landing zone setup	Read	LandingZone*		
GetLandingZoneDriftStatus	Grants permission to get the current landing zone drift status	Read			
GetLandingZoneOperation	Grants permission to get the current status of a particular landing zone operation	Read			
GetLandingZoneStatus [permission only]	Grants permission to get the current status of the landing zone setup	Read			
ListBaselines	Grants permission to list Baselines	List			
ListControlOperations	Grants permission to list all control operations	List			
ListDirectoryGroups [permission only]	Grants permission to list the current directory groups available through IAM Identity Center	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDriftDetails	Grants permission to list occurrences of drift in AWS Control Tower	Read			
ListEnabledBaselines	Grants permission to list enabled Baselines	List			
ListEnabledControls	Grants permission to list all enabled controls in a specified organizational unit	List			
ListEnabledGuardrails [permission only]	Grants permission to list currently enabled guardrails	List			
ListExtendedGovernancePrecheckDetails [permission only]	Grants permission to list Precheck details for an Organizational Unit	List			
ListExternalConfigRuleCompliance	Grants permission to list the compliance of external AWS Config rules	Read			
ListGuardrailViolations [permission only]	Grants permission to list existing guardrail violations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGuardrails [permission only]	Grants permission to list all available guardrails	List			
ListGuardrailsForTarget [permission only]	Grants permission to list guardrails and their current state for a organizational unit	List			
ListLandingZoneOperations	Grants permission to list all landing zone operations	List			
ListLandingZones	Grants permission to list all landing zones	List			
ListManagedAccounts [permission only]	Grants permission to list accounts managed through AWS Control Tower	List			
ListManagedAccountsForGuardrail [permission only]	Grants permission to list managed accounts with a specified guardrail applied	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListManagedAccountsForParent [permission only]	Grants permission to list managed accounts under an organizational unit	List			
ListManagedOrganizationalUnits [permission only]	Grants permission to list organizational units managed by AWS Control Tower	List			
ListManagedOrganizationalUnitsForGuardrail [permission only]	Grants permission to list managed organizational units that have a specified guardrail applied	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	EnabledBaseline		
			EnabledControl		
			LandingZone		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ManageOrganizationalUnit [permission only]	Grants permission to set up an organizational unit to be managed by AWS Control Tower	Write			
PerformPreLaunchChecks [permission only]	Grants permission to perform validations in an account	Read			
ResetEnabledBaseline	Grants permission to reset an enabled Baseline	Write	EnabledBaseline*		
ResetEnabledControl	Grants permission to reset an enabled control for an organizational unit	Write	EnabledControl*		
ResetLandingZone	Grants permission to reset a landing zone	Write	LandingZone*		
SetupLandingZone [permission only]	Grants permission to set up or update AWS Control Tower landing zone	Write			
TagResource	Grants permission to add tags to a resource	Tagging	EnabledBaseline		
			EnabledControl		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			LandingZone		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	EnabledBaseline		
			EnabledControl		
			LandingZone		
				aws:TagKeys	
UpdateAccountFactoryConfig [permission only]	Grants permission to update the account factory configuration	Write			
UpdateEnabledBaseline	Grants permission to update an enabled Baseline	Write	EnabledBaseline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnabledControl	Grants permission to update an enabled control for an organizational unit	Write	EnabledControl*		
UpdateLandingZone	Grants permission to update a landing zone	Write	LandingZone*		

Resource types defined by AWS Control Tower

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
EnabledControl	`arn:${Partition}:controltower:${Region}:${Account}:enabledcontrol/${EnabledControlId}`	aws:ResourceTag/${TagKey}
Baseline	`arn:${Partition}:controltower:${Region}::baseline/${BaselineId}`	
EnabledBaseline	`arn:${Partition}:controltower:${Region}:${Account}:enabledbaseline/${EnabledBaselineId}`	aws:ResourceTag/${TagKey}
LandingZone	`arn:${Partition}:controltower:${Region}:${Account}:landingzone/${LandingZoneId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Control Tower

AWS Control Tower defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Cost and Usage Report

AWS 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 AWS Cost and Usage Report
- Resource types defined by AWS Cost and Usage Report
- Condition keys for AWS Cost and Usage Report

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS services, usage type and operation for the Usage Report workflow. Allows or denies download of usage reports too	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a resource	Read	cur*		
				aws:ResourceTag/${TagKey}	
ModifyReportDefinition	Grants permission to modify Cost and Usage Report Definition	Write	cur*		
PutClassicReportPreferences [permission only]	Grants permission to enable classic reports	Write			
PutReportDefinition	Grants permission to write Cost and Usage Report Definition	Write	cur*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a resource	Tagging	cur*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	cur*		
				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 AWS 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 AWS Cost and Usage Report

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Cost Explorer Service

AWS Cost Explorer Service (service prefix: `ce`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Cost Explorer Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAnomalyMonitor	Grants permission to create a new Anomaly Monitor	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	Grants permission to create a new Anomaly Subscription	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateCostCategoryDefinition	Grants permission to create a new Cost Category with the requested name and rules	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscription [permission only]	Grants permission to create Reservation expiration alerts	Write			
CreateReport [permission only]	Grants permission to create Cost Explorer Reports	Write			
DeleteAnomalyMonitor	Grants permission to delete an Anomaly Monitor	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Grants permission to delete an Anomaly Subscription	Write	anomalysubscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Grants permission to delete a Cost Category	Write	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [permission only]	Grants permission to delete Reservation expiration alerts	Write			
DeleteReport [permission only]	Grants permission to delete Cost Explorer Reports	Write			
DescribeCostCategoryDefinition	Grants permission to retrieve descriptions such as the name, ARN, rules, definition, and effective dates of a Cost Category	Read	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNotificationSubscription [permission only]	Grants permission to view Reservation expiration alerts	Read			
DescribeReport [permission only]	Grants permission to view Cost Explorer Reports page	Read			
GetAnomalies	Grants permission to retrieve anomalies	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Grants permission to query Anomaly Monitors	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	Grants permission to query Anomaly Subscriptions	Read	anomalysubscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	Grants permission to retrieve approximate usage record count for the chosen resource, level, and hourly granularity preferences, derived from the past month's usage	Read			
GetCommitmentPurchaseAnalysis	Grants permission to retrieve the commitment purchase analysis for your account	Read			
GetConsoleActionSetEnforced [permission only]	Grants permission to view whether existing or fine-grained IAM actions are being used to control authorization to Billing, Cost Management, and Account consoles	Read			
GetCostAndUsage	Grants permission to retrieve the cost and usage metrics for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCostAndUsageComparisons	Grants permission to retrieve the cost and usage comparisons for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageWithResources	Grants permission to retrieve the cost and usage metrics with resources for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	Grants permission to query Cost Catagory names and values for a specified time period	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostComparisonDrivers	Grants permission to retrieve the cost drivers for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCostForecast	Grants permission to retrieve a cost forecast for a forecast time period	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetDimensionValues	Grants permission to retrieve all available filter values for a filter for a period of time	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetPreferences [permission only]	Grants permission to view Cost Explorer Preferences page	Read			
GetReservationCoverage	Grants permission to retrieve the reservation coverage for your account	Read			
GetReservationPurchaseRecommendation	Grants permission to retrieve the reservation recommendations for your account	Read			
GetReservationUtilization	Grants permission to retrieve the reservation utilization for your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRightsizingRecommendation	Grants permission to retrieve the rightsizing recommendations for your account	Read			
GetSavingsPlanPurchaseRecommendationDetails	Grants permission to retrieve the Savings Plan recommendation details for your account	Read			
GetSavingsPlansCoverage	Grants permission to retrieve the Savings Plans coverage for your account	Read			
GetSavingsPlansPurchaseRecommendation	Grants permission to retrieve the Savings Plans recommendations for your account	Read			
GetSavingsPlansUtilization	Grants permission to retrieve the Savings Plans utilization for your account	Read			
GetSavingsPlansUtilizationDetails	Grants permission to retrieve the Savings Plans utilization details for your account	Read			
GetTags	Grants permission to query tags for a specified time period	Read	billingview		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetUsageForecast	Grants permission to retrieve a usage forecast for a forecast time period	Read	billingview		
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	Grants permission to retrieve a list of your historical commitment purchase analyses	List			
ListCostAllocationTagBackfillHistory	Grants permission to list Cost Allocation Tag backfill history	List			
ListCostAllocationTags	Grants permission to list Cost Allocation Tags	List			
ListCostCategoryDefinitions	Grants permission to retrieve names, ARN, and effective dates for all Cost Categories	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCostCategoryResourceAssociations	Grants permission to retrieve resource associations of all Cost Categories defined in the account	List			
ListSavingsPlansPurchaseRecommendationGeneration	Grants permission to retrieve a list of your historical recommendation generations	List			
ListTagsForResource	Grants permission to list tags for a Cost Explorer resource	Read	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	Grants permission to provide feedback on detected anomalies	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCommitmentPurchaseAnalysis	Grants permission to request a commitment purchase analysis	Write			
StartCostAllocationTagBackfill	Grants permission to request a Cost Allocation Tag backfill	Write			
StartSavingsPlansPurchaseRecommendationGeneration	Grants permission to request a Savings Plans recommendation generation	Write			
TagResource	Grants permission to tag a Cost Explorer resource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from a Cost Explorer resource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	Grants permission to update an existing Anomaly Monitor	Write	anomalymonitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	Grants permission to update an existing Anomaly Subscription	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [permission only]	Grants permission to change whether existing or fine-grained IAM actions will be used to control authorization to Billing, Cost Management, and Account consoles	Write			
UpdateCostAllocationTagsStatus	Grants permission to update existing Cost Allocation Tags status	Write			
UpdateCostCategoryDefinition	Grants permission to update an existing Cost Category	Write	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotification Subscription [permission only]	Grants permission to update Reservation expiration alerts	Write			
UpdatePreferences [permission only]	Grants permission to edit Cost Explorer Preferences page	Write			
UpdateReport [permission only]	Grants permission to update Cost Explorer Reports	Write			

Resource types defined by AWS Cost Explorer Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
anomalysubscription	`arn:${Partition}:ce::${Account}:anomalysubscription/${Identifier}`	aws:ResourceTag/${TagKey}
anomalymonitor	`arn:${Partition}:ce::${Account}:anomalymonitor/${Identifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
costcategory	arn:${Partition}:ce::${Account}:costcategory/${Identifier}	aws:ResourceTag/${TagKey}
billingview	arn:${Partition}:billing::${Account}:billingview/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Cost Explorer Service

AWS Cost Explorer Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Cost Optimization Hub

AWS Cost Optimization Hub (service prefix: cost-optimization-hub) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Cost Optimization Hub

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPreferences	Grants permission to get preferences	Read			
GetRecommendation	Grants permission to get resource configuration and estimated cost impact for a recommendation	Read			
ListEfficiencyMetrics	Grants permission to list efficiency metric scores by group	List			
ListEnrollmentStatuses	Grants permission to list enrollment statuses for the specified account or all members under a management account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecommendationSummaries	Grants permission to list recommendation summaries by group	List			cost-optimization-hub:GetRecommendation
ListRecommendations	Grants permission to list summary view of recommendations	List			cost-optimization-hub:GetRecommendation
UpdateEnrollmentStatus	Grants permission to update the enrollment status	Write			
UpdatePreferences	Grants permission to update preferences	Write			

Resource types defined by AWS Cost Optimization Hub

AWS Cost Optimization Hub does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Cost Optimization Hub, specify `"Resource": "*"` in your policy.

Condition keys for AWS Cost Optimization Hub

Cost Optimization Hub has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Customer Verification Service

AWS Customer Verification Service (service prefix: `customer-verification`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Customer Verification Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action

with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomerVerificationDetails [permission only]	Grants permission to create customer verification data	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUploadUrls [permission only]	Grants permission to create upload URLs	Write			
GetCustomerVerificationDetails [permission only]	Grants permission to get customer verification data	Read			
GetCustomerVerificationEligibility [permission only]	Grants permission to get customer verification eligibility	Read			
UpdateCustomerVerificationDetails [permission only]	Grants permission to update customer verification data	Write			

Resource types defined by AWS Customer Verification Service

AWS Customer Verification Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Customer Verification Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Customer Verification Service

Customer Verification 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Data Exchange

AWS Data Exchange (service prefix: `dataexchange`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Data Exchange
- Resource types defined by AWS Data Exchange
- Condition keys for AWS Data Exchange

Actions defined by AWS Data Exchange

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDataGrant	Grants permission to accept a data grant	Write	data-grants*		
CancelJob	Grants permission to cancel a job	Write	jobs*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAsset [permission only]	Grants permission to create an asset (for example, in a Job)	Write	revisions*		
CreateDataGrant	Grants permission to create a data grant	Write	data-grants*		dataexchange:PublishToDataGrant
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Grants permission to create a data set	Write	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventAction	Grants permission to create an event action	Write	event-actions*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Grants permission to create a job to import or export assets	Write	jobs*		
				dataexchange:JobType	
CreateRevision	Grants permission to create a revision	Write	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAsset	Grants permission to delete an asset	Write	assets*		
DeleteDataGrant	Grants permission to delete a data grant	Write	data-grants*		
DeleteDataSet	Grants permission to delete a data set	Write	data-sets*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			entitled-data-sets*		
DeleteEventAction	Grants permission to delete an event action	Write	event-actions*		
DeleteRevision	Grants permission to delete a revision	Write	revisions*		
GetAsset	Grants permission to get information about an asset and to export it (for example, in a Job)	Read	assets*		
			entitled-assets*		
GetDataGrant	Grants permission to get a data grant	Read	data-grants*		
GetDataSet	Grants permission to get information about a data set	Read	data-sets*		
			entitled-data-sets*		
GetEventAction	Grants permission to get an event action	Read	event-actions*		
GetJob	Grants permission to get information about a job	Read	jobs*		
GetReceivedDataGrant	Grants permission to get a received data grant	Read	data-grants*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRevision	Grants permission to get information about a revision	Read	entitled-revisions *		
			revisions *		
ListDataGrants	Grants permission to list data grants for the account	List			
ListDataSetRevisions	Grants permission to list the revisions of a data set	List	data-sets *		
			entitled-data-sets *		
ListDataSets	Grants permission to list data sets for the account	List			
ListEventActions	Grants permission to list event actions for the account	List			
ListJobs	Grants permission to list jobs for the account	List			
ListReceivedDataGrants	Grants permission to list received data grants for the account	List			
ListRevisionAssets	Grants permission to get list the assets of a revision	List	entitled-revisions *		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			revisions*		
ListTagsForResource	Grants permission to list the tags that you associated with the specified resource	List	data-grants		
			data-sets		
			event-actions		
			revisions		
PublishDataSet [permission only]	Grants permission to publish a data set to a product	Write	data-sets*		
PublishToDataGrant [permission only]	Grants permission to publish a data set to a data grant	Write	data-sets*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RevokeRevision	Grants permission to revoke subscriber access to a revision	Write	revisions*		
SendApiAsset	Grants permission to send a request to an API asset	Write	assets*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			entitled-assets*		
SendDataSetNotification	Grants permission to send a notification to subscribers of a data set	Write	data-sets*		
StartJob	Grants permission to start a job	Write	jobs*		dataexchange:CreateAsset dataexchange:DeleteDataSet dataexchange:GetAsset dataexchange:GetDataSet dataexchange:GetRevision dataexchange:PublishDataSet redshift:AuthorizeDataShare

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add one or more tags to a specified resource	Tagging	data-grants		
			data-sets		
			event-actions		
			revisions		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a specified resource	Tagging	data-grants		
			data-sets		
			event-actions		
			revisions		
				aws:TagKeys	
UpdateAsset	Grants permission to get update information about an asset	Write	assets*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataSet	Grants permission to update information about a data set	Write	data-sets*		
UpdateEventAction	Grants permission to update information for an event action	Write	event-actions*		
UpdateRevision	Grants permission to update information about a revision	Write	revisions*		dataexchange:PublishDataSet dataexchange:PublishToDataGrant

Resource types defined by AWS Data Exchange

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
jobs	`arn:${Partition}:dataexchange:${Region}:${Account}:jobs/${JobId}`	dataexchange:JobType

Resource types	ARN	Condition keys
data-sets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}	aws:ResourceTag/${TagKey}
entitled-data-sets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}	
revisions	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}	aws:ResourceTag/${TagKey}
entitled-revisions	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}	
assets	arn:${Partition}:dataexchange:${Region}:${Account}:data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
entitled-assets	arn:${Partition}:dataexchange:${Region}::data-sets/${DataSetId}/revisions/${RevisionId}/assets/${AssetId}	
event-actions	arn:${Partition}:dataexchange:${Region}:${Account}:event-actions/${EventActionId}	aws:ResourceTag/${TagKey}
data-grants	arn:${Partition}:dataexchange:${Region}:${Account}:data-grants/${DataGrantId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Data Exchange

AWS Data Exchange defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the mandatory tags in the create request	String
aws:ResourceTag/${TagKey}	Filters access by the tag value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the create request	ArrayOfString
dataexchange:JobType	Filters access by the specified job type	String

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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLifecyclePolicy	Grants permission to create a data lifecycle policy to manage the scheduled creation and retention of Amazon EBS snapshots. You may have up to 100 policies	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	Grants permission to delete an existing data lifecycle policy. In addition, this action halts the creation and deletion of snapshots that 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	policy*		
TagResource	Grants permission to add or update tags of a resource	Tagging	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	Grants permission to update an existing data lifecycle policy	Write	policy*		

Resource types defined by Amazon Data Lifecycle Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Data Pipeline

AWS Data Pipeline (service prefix: `datapipeline`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Data Pipeline

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivatePipeline	Grants permission to validate the specified pipeline and starts processing pipeline tasks. If the pipeline does not pass validation, activation fails	Write	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
AddTags	Grants permission to add or modify tags for the specified pipeline	Tagging	pipeline*		
				datapipeline:Pipel	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
CreatePipeline	Grants permission to create a new, empty pipeline	Write		aws:RequestTag/${TagKey} aws:TagKeys datapipeline:Tag/${TagKey}	datapipeline:AddTags
DeactivatePipeline	Grants permission to Deactivate the specified running pipeline	Write	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
DeletePipeline	Grants permission to delete a pipeline, its pipeline definition, and its run history	Write	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
DescribeObjects	Grants permission to get the object definitions for a set of objects associated with the pipeline	Read	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePipelines	Grants permission to retrieves metadata about one or more pipelines	Read	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
EvaluateExpression	Grants permission to task runners to call EvaluateExpression, to evaluate a string in the context of the specified object	Read	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
GetAccountLimits [permission only]	Grants permission to call GetAccountLimits	List			
GetPipelineDefinition	Grants permission to gets the definition of the specified pipeline	Read	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
ListPipelines	Grants permission to list the pipeline identifiers for all active pipelines that you have permission to access	List			
PollForTask	Grants permission to task runners to call PollForTask, to receive a task to perform from AWS Data Pipeline	Write		datapipeline:workerGroup	
PutAccountLimits [permission only]	Grants permission to call PutAccountLimits	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPipelineDefinition	Grants permission to add tasks, schedules, and preconditions to the specified pipeline	Write	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	
QueryObjects	Grants permission to query the specified pipeline for the names of objects that match the specified set of conditions	Read	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
RemoveTags	Grants permission to remove existing tags from the specified pipeline	Tagging	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
ReportTaskProgress	Grants permission to task runners to call ReportTaskProgress, when they are assigned a task to acknowledge that it has the task	Write	pipeline*		
ReportTaskRunnerHeartbeat	Grants permission to task runners to call ReportTaskRunnerHeartbeat every 15 minutes to indicate that they are operational	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetStatus	Grants permission to requests that the status of the specified physical or logical pipeline objects be updated in the specified pipeline	Write	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey}	
SetTaskStatus	Grants permission to task runners to call SetTaskStatus to notify AWS Data Pipeline that a task is completed and provide information about the final status	Write	pipeline*		
ValidatePipelineDefinition	Grants permission to validate the specified pipeline definition to ensure that it is well formed and can be run without error	Read	pipeline*		
				datapipeline:PipelineCreator datapipeline:Tag/${TagKey} datapipeline:workerGroup	

Resource types defined by AWS Data Pipeline

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
pipeline	`arn:${Partition}:datapipeline:${Region}:${Account}:pipeline/${PipelineId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Data Pipeline

AWS Data Pipeline defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Condition keys	Description	Type
datapipeline:PipelineCreator	Filters access by the IAM user that created the pipeline	ArrayOfString
datapipeline:Tag/${TagKey}	Filters access by customer-specified key/value pair that can be attached to a resource	String
datapipeline:workerGroup	Filters access by the name of a worker group for which a Task Runner retrieves work	ArrayOfString

Actions, resources, and condition keys for AWS Database Migration Service

AWS 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 AWS Database Migration Service
- Resource types defined by AWS Database Migration Service
- Condition keys for AWS Database Migration Service

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
CancelMetadataModelConversion	Grants permission to cancel a single metadata model conversion operation that was started with StartMetadataModelConversion	Write	MigrationProject*		
CancelMetadataModelCreation	Grants permission to cancel a single metadata model creation operation that was started with StartMetadataModelCreation	Write	MigrationProject*		
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 AWS 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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOutboundIntegration [permission only]	Grants permission to DMS to create resources for zero-ETL integrations with self managed databases	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
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 AWS 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 AWS 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
DescribeMetadataModel	Grants permission to get detailed information about the specified metadata model, including its definition and corresponding converted objects in the target database if applicable	Read	Migration Project*		
DescribeMetadataModelChildren	Grants permission to get a list of child metadata models for the specified metadata model in the database hierarchy	Read	Migration Project*		
DescribeMetadataModelCreations	Grants permission to return a paginated list of metadata model creation requests for a migration project	Read	Migration Project*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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*		
DescribeReplicationConfigs	Grants permission to describe replication configs	Read			
DescribeReplicationInstanceTaskLogs	Grants permission to return information about the task logs for the specified task	Read	ReplicationInstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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			
DescribeSchemas	Grants permission to return information about the schema for the specified endpoint	Read	Endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
GetTargetSelectionRules	Grants permission to convert source selection rules into their target counterparts for schema conversion operations	Read	MigrationProject*		
ImportCertificate	Grants permission to upload the specified certificate	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	Grants permission to list the AWS DMS attributes for a data providers	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExtensionPacks	Grants permission to list the AWS DMS attributes for a extension packs	Read	MigrationProject		
ListInstanceProfiles	Grants permission to list the AWS DMS attributes for a instance profiles	Read	InstanceProfile		
ListMetadataModelAssessmentActionItems [permission only]	Grants permission to list the AWS 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	MigrationProject		dms:StartMetadataModelImport
ListMetadataModelAssessments	Grants permission to list the AWS DMS attributes for a metadata model assessments	Read	MigrationProject		
ListMetadataModelConversions	Grants permission to list the AWS DMS attributes for a metadata model conversions	Read	MigrationProject		
ListMetadataModelExports	Grants permission to list the AWS DMS attributes for a metadata model exports	Read	MigrationProject		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMigrationProjects	Grants permission to list the AWS 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 AWS 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		
ModifyEventSubscription	Grants permission to modify an existing AWS DMS event notification subscription	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ModifyOutboundIntegration [permission only]	Grants permission to DMS to modify resources for zero-ETL integrations with self managed databases	Write			iam:PassRole
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*		
StartMetadataModelCreation	Grants permission to create source metadata model of the given type with the specified properties for schema conversion operations	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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartReplicationTask	Grants permission to start the replication task	Write	ReplicationTask*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataProvider	Grants permission to update the specified data provider	Write	DataProvider*		
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 AWS 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} 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 AWS Database Migration Service

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 Database Query Metadata Service

Database Query Metadata Service (service prefix: `dbqms`) 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 Database Query Metadata Service
- Resource types defined by Database Query Metadata Service
- Condition keys for Database Query Metadata Service

Actions defined by Database Query Metadata Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFavoriteQuery	Grants permission to create a new favorite query	Write			
CreateQueryHistory	Grants permission to add a query to the history	Write			
CreateTab	Grants permission to create a new query tab	Write			
DeleteFavoriteQueries	Grants permission to delete saved queries	Write			
DeleteQueryHistory	Grants permission to delete a historical query	Write			
DeleteTab	Grants permission to delete query tab	Write			
DescribeFavoriteQueries	Grants permission to list saved queries and associated metadata	List			
DescribeQueryHistory	Grants permission to list history of queries that were run	List			
DescribeTabs	Grants permission to list query tabs and associated metadata	List			
GetQueryString	Grants permission to retrieve favorite or history query string by id	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFavoriteQuery	Grants permission to update saved query and description	Write			
UpdateQueryHistory	Grants permission to update the query history	Write			
UpdateTab	Grants permission to update query tab	Write			

Resource types defined by Database Query Metadata Service

Database Query Metadata Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Database Query Metadata Service, specify `"Resource": "*"` in your policy.

Condition keys for Database Query Metadata Service

DBQMS has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS DataSync

AWS DataSync (service prefix: `datasync`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS DataSync
- Resource types defined by AWS DataSync
- Condition keys for AWS DataSync

Actions defined by AWS DataSync

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddStorageSystem	Grants permission to create a storage system	Write	agent*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CancelTaskExecution	Grants permission to cancel execution of a sync task	Write	taskexecution*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAgent	Grants permission to activate an agent that you have deployed on your host	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Grants permission to create an endpoint for a Microsoft Azure Blob Storage container	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationEfs	Grants permission to create an endpoint for an Amazon EFS file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxLustre	Grants permission to create an endpoint for an Amazon Fsx Lustre	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocationFsxOntap	Grants permission to create an endpoint for Amazon FSx for ONTAP	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Grants permission to create an endpoint for Amazon FSx for OpenZFS	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxWindows	Grants permission to create an endpoint for an Amazon FSx Windows File Server file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationHdfs	Grants permission to create an endpoint for an Amazon Hdfs	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocationNfs	Grants permission to create an endpoint for a NFS file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationObjectStorage	Grants permission to create an endpoint for a self-managed object storage bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationS3	Grants permission to create an endpoint for an Amazon S3 bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationSmb	Grants permission to create an endpoint for an SMB file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTask	Grants permission to create a sync task	Write	location*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			agent		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Grants permission to delete an agent	Write	agent*		
DeleteLocation	Grants permission to delete a location used by AWS DataSync	Write	location*		
DeleteTask	Grants permission to delete a sync task	Write	task*		
DescribeAgent	Grants permission to view metadata such as name, network interfaces, and the status (that is, whether the agent is running or not) about a sync agent	Read	agent*		
DescribeDiscoveryJob	Grants permission to describe metadata about a discovery job	Read	discovery job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocationAzureBlob	Grants permission to view metadata, such as the path information about an Azure Blob Storage sync location	Read	location*		
DescribeLocationEfs	Grants permission to view metadata, such as the path information about an Amazon EFS sync location	Read	location*		
DescribeLocationFsxLustre	Grants permission to view metadata, such as the path information about an Amazon FSx Lustre sync location	Read	location*		
DescribeLocationFsxOntap	Grants permission to view metadata, such as the path information about an Amazon FSx for ONTAP sync location	Read	location*		
DescribeLocationFsxOpenZfs	Grants permission to view metadata, such as the path information about an Amazon FSx OpenZFS sync location	Read	location*		
DescribeLocationFsxWindows	Grants permission to view metadata, such as the path information about an Amazon FSx Windows sync location	Read	location*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocationHdfs	Grants permission to view metadata, such as the path information about an Amazon HDFS sync location	Read	location*		
DescribeLocationNfs	Grants permission to view metadata, such as the path information, about a NFS sync location	Read	location*		
DescribeLocationObjectStorage	Grants permission to view metadata about a self-managed object storage server location	Read	location*		
DescribeLocationS3	Grants permission to view metadata, such as bucket name, about an Amazon S3 bucket sync location	Read	location*		
DescribeLocationSmb	Grants permission to view metadata, such as the path information, about an SMB sync location	Read	location*		
DescribeStorageSystem	Grants permission to view metadata about a storage system	Read	storagesystem*		
DescribeStorageSystemResourceMetrics	Grants permission to describe resource metrics collected by a discovery job	List	discoveryjob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStorageSystemResources	Grants permission to describe resources identified by a discovery job	List	discoveryjob*		
DescribeTask	Grants permission to view metadata about a sync task	Read	task*		
DescribeTaskExecution	Grants permission to view metadata about a sync task that is being executed	Read	taskexecution*		
				aws:ResourceTag/${TagKey}	
GenerateRecommendations	Grants permission to generate recommendations for a resource identified by a discovery job	Write	discoveryjob*		
ListAgents	Grants permission to list agents owned by an AWS account in a region specified in the request	List			
ListDiscoveryJobs	Grants permission to list discovery jobs	List			
ListLocations	Grants permission to list source and destination sync locations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStorageSystems	Grants permission to list storage systems	List			
ListTagsForResource	Grants permission to list tags that have been added to the specified resource	Read	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
ListTaskExecutions	Grants permission to list executed sync tasks	List		aws:ResourceTag/${TagKey}	
ListTasks	Grants permission to list of all the sync tasks	List			
RemoveStorageSystem	Grants permission to delete a storage system	Write	storagesystem*		
StartDiscoveryJob	Grants permission to start a discovery job for a storage system	Write	storagesystem*		
StartTaskExecution		Write	task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to start a specific invocation of a sync task			aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	Grants permission to stop a discovery job	Write	discoveryjob*		
TagResource	Grants permission to apply a key-value pair to an AWS resource	Tagging	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:TagKeys	
UpdateAgent	Grants permission to update the name of an agent	Write	agent*		
UpdateDiscoveryJob	Grants permission to update a discovery job	Write	discoveryjob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLocationAzureBlob	Grants permission to update an Azure Blob Storage sync location	Write	location*		
UpdateLocationEfs	Grants permission to update an EFS sync Location	Write	location*		
UpdateLocationFsxLustre	Grants permission to update an FSx Lustre sync Location	Write	location*		
UpdateLocationFsxOntap	Grants permission to update an FSx ONTAP sync Location	Write	location*		
UpdateLocationFsxOpenZfs	Grants permission to update an FSx OpenZFS sync Location	Write	location*		
UpdateLocationFsxWindows	Grants permission to update an FSx Windows sync Location	Write	location*		
UpdateLocationHdfs	Grants permission to update an HDFS sync Location	Write	location*		
UpdateLocationNfs	Grants permission to update an NFS sync Location	Write	location*		
UpdateLocationObjectStorage	Grants permission to update a self-managed object storage server location	Write	location*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLocationS3	Grants permission to update an S3 sync Location	Write	location*		
UpdateLocationSmb	Grants permission to update a SMB sync location	Write	location*		
UpdateStorageSystem	Grants permission to update a storage system	Write	storagesystem*		
UpdateTask	Grants permission to update metadata associated with a sync task	Write	task*		
UpdateTaskExecution	Grants permission to update execution of a sync task	Write	taskexecution*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS DataSync

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
agent	arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}	aws:ResourceTag/${TagKey}
location	arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}	aws:ResourceTag/${TagKey}
task	arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}	aws:ResourceTag/${TagKey}
taskexecution	arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}	aws:ResourceTag/${TagKey}
storagesystem	arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}	aws:ResourceTag/${TagKey}
discoveryjob	arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}	aws:ResourceTag/${TagKey}

Condition keys for AWS DataSync

AWS DataSync defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs associated with the resource	String
aws:TagKeys	Filters access by the tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon DataZone

Amazon DataZone (service prefix: `datazone`) 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 DataZone
- Resource types defined by Amazon DataZone
- Condition keys for Amazon DataZone

Actions defined by Amazon DataZone

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptPredictions	Grants permission to accept prediction	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptSubscriptionRequest	Grants permission to approve a subscription request for a Data Asset	Write			
AddEntityOwner	Grants permission to add an owner to an entity like domain unit	Write			
AddPolicyGrant	Grants permission to add a policy grant	Permissions management			
AssociateEnvironmentRole	Grants permission to associate a role in a default service blueprint environment	Write			
AssociateGovernedTerms	Grants permission to associate governed terms to an asset	Write			
BatchDeleteLinkedTypes [permission only]	Grants permission to remove linked type items from an Amazon DataZone Domain	Write	domain*		
BatchGetAttributesMetadata	Grants permission to retrieve attributes metadata	Read			
BatchGetCell	Grants permission to batch get cells	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetCellRun	Grants permission to batch get cell runs	Read			
BatchPutAttributesMetadata	Grants permission to create and update attributes metadata	Write			
BatchPutLinkedTypes [permission only]	Grants permission to put linked type items to an Amazon DataZone Domain	Write	domain*		
CancelMetadataGenerationRun	Grants permission to cancel metadata generation run	Write			
CancelSubscription	Grants permission to revoke or unsubscribe an approved subscription to Data Asset	Write			
CreateAccountPool	Grants permission to create an account pool	Write			
CreateAsset	Grants permission to create asset	Write			
CreateAssetFilter	Grants permission to create asset filter	Write			
CreateAssetRevision	Grants permission to create new revision of an asset	Write			
CreateAssetType	Grants permission to create an asset type	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCell	Grants permission to create cells	Write			
CreateCellRun	Grants permission to create cell runs	Write			
CreateConnection	Grants permission to create connections	Write			
CreateDataProduct	Grants permission to create data product	Write			
CreateDataProductRevision	Grants permission to create data product revision	Write			
CreateDataSource	Grants permission to create a new DataSource	Write			
CreateDomain	Grants permission to provision a domain which is a top level entity that contains other Amazon DataZone resources	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainUnit	Grants permission to create a domain unit	Write			
CreateEnvironment	Grants permission to create a collection of configurated resources used to publish and subscribe to data	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironmentAction	Grants permission to create an environment action in a default service blueprint environment	Write			
CreateEnvironmentBlueprint	Grants permission to create a custom Environment Blueprint that allow user to add Environments to their Project	Write			
CreateEnvironmentProfile	Grants permission to create a template from a Blueprint that can be used to create a Environment	Write			
CreateFormType	Grants permission to create a form type or a new revision of it	Write			
CreateGlossary	Grants permission to create a business glossary	Write			
CreateGlossaryTerm	Grants permission to create a glossary term	Write			
CreateGroupProfile	Grants permission to create a DataZone group profile for an IAM Identity Center group	Write			
CreateListingChangeSet	Grants permission to create listing change set	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNotebook	Grants permission to create notebooks	Write			
CreateProject	Grants permission to create a Project to enable your team to publish and subscribe to data	Write			
CreateProjectMembership	Grants permission to add a user to a Project	Write			
CreateProjectProfile	Grants permission to create a project profile	Write			
CreateRule	Grants permission to create rule	Write			
CreateSubscriptionGrant	Grants permission to create a grant for an approved subscription on a subscription target	Write			
CreateSubscriptionRequest	Grants permission to create a subscription request for a Data Asset	Write			
CreateSubscriptionTarget	Grants permission to create a subscription target for a Environment in the project	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUserProfile	Grants permission to create a user profile for an existing user in the customers IAM Identity Center	Write			
DeleteAccountPool	Grants permission to delete an account pool	Write			
DeleteAsset	Grants permission to delete an asset	Write			
DeleteAssetFilter	Grants permission to delete asset filter	Write			
DeleteAssetType	Grants permission to delete an asset type	Write			
DeleteCell	Grants permission to delete cells	Write			
DeleteCellRun	Grants permission to delete cell runs	Write			
DeleteConnection	Grants permission to delete connections	Write			
DeleteDataExportConfiguration	Grants permission to delete DataZone catalog data export configuration	Write			
DeleteDataProduct	Grants permission to delete data product	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDataSource	Grants permission to update existing DataSource	Write			
DeleteDomain	Grants permission to delete a provisioned domain	Write	domain*		
DeleteDomainSharingPolicy [permission only]	Grants permission to delete a resource policy for a DataZone Domain	Permissions management			
DeleteDomainUnit	Grants permission to delete an existing domain unit	Write			
DeleteEnvironment	Grants permission to Delete Environment	Write			
DeleteEnvironmentAction	Grants permission to delete an environment action in a default service blueprint environment	Write			
DeleteEnvironmentBlueprint	Grants permission to delete Environment Blueprint	Write			
DeleteEnvironmentBlueprintConfiguration	Grants permission to delete environment blueprint configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEnvironmentProfile	Grants permission to delete Environment Profile	Write			
DeleteFormType	Grants permission to delete a form type	Write			
DeleteGlossary	Grants permission to delete a business glossary	Write			
DeleteGlossaryTerm	Grants permission to delete a glossary term	Write			
DeleteListing	Grants permission to delete listing	Write			
DeleteNotebook	Grants permission to delete notebooks	Write			
DeleteProject	Grants permission to delete a Project that enables your team to publish and subscribe to data	Write			
DeleteProjectMembership	Grants permission to remove a user from a project	Write			
DeleteProjectProfile	Grants permission to delete a project profile	Write			
DeleteRule	Grants permission to delete rule	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubscriptionGrant	Grants permission to delete a subscription grant from a subscription target	Write			
DeleteSubscriptionRequest	Grants permission to delete a pending subscription request for a Data Asset	Write			
DeleteSubscriptionTarget	Grants permission to delete a subscription target from a Environment in the project	Write			
DeleteTimeSeriesDataPoints	Grants permission to delete existing TimeSeriesDataPoints	Write			
DisassociateEnvironmentRole	Grants permission to disassociate a role in a default service blueprint environment	Write			
DisassociateGovernedTerms	Grants permission to disassociate governed terms to an asset	Write			
GenerateCode	Grants permission to generate code	Write			
GetAccountPool	Grants permission to get account pool details	Read			
GetAsset	Grants permission to retrieve an asset	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssetFilter	Grants permission to get asset filter	Read			
GetAssetType	Grants permission to get an asset type	Read			
GetCell	Grants permission to get cells	Read			
GetCellRun	Grants permission to get cell runs	Read			
GetCellRunResult	Grants permission to get cell run result	Read			
GetConnection	Grants permission to get connections	Read			
GetConversation	Grants permission to get conversations	Read			
GetDataExportConfiguration	Grants permission to retrieve DataZone catalog data export configuration	Read			
GetDataProduct	Grants permission to get data product	Read			
GetDataSource	Grants permission to Get a existing DataSource in Amazon DataZone using its identifier	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataSourceRun	Grants permission to get DataSource run job in Amazon DataZone using it's identifier	Read			
GetDomain	Grants permission to retrieve information about a domain	Read	domain*		
GetDomainExecutionRoleCredentials [permission only]	Grants permission to use features that require access to domain execution role credentials	Read			
GetDomainSharingPolicy [permission only]	Grants permission to retrieve a resource policy for a DataZone Domain	Read			
GetDomainUnit	Grants permission to get an existing domain unit	Read			
GetEnvironment	Grants permission to get Environment details	Read			
GetEnvironmentAction	Grants permission to get an environment action in a default service blueprint environment	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEnvironmentActionLink [permission only]	Grants permission to get environment action link	Read			
GetEnvironmentBlueprint	Grants permission to get Environment Blueprint details	Read			
GetEnvironmentBlueprintConfiguration	Grants permission to get environment blueprint configuration	Read			
GetEnvironmentCredentials	Grants permission to get short term credentials that assume the Environment user role	Read			
GetEnvironmentProfile	Grants permission to get Environment Profile details	Read			
GetFormType	Grants permission to get a form type	Read			
GetGlossary	Grants permission to get a business glossary	Read			
GetGlossaryTerm	Grants permission to get a glossary term	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupProfile	Grants permission to retrieve an existing DataZone group profile	Read			
GetIamPortalLoginUrl	Grants permission to an IAM principal to log into the DataZone Portal	Permissions management			
GetJobRun	Grants permission to get job runs	Read			
GetLineageEvent	Grants permission to get lineage events	Read			
GetLineageNode	Grants permission to get the lineage node	Read			
GetListing	Grants permission to get listing	Read			
GetMetadataGenerationRun	Grants permission to get metadata generation run	Read			
GetNotebook	Grants permission to get notebooks	Read			
GetNotebookCompute	Grants permission to get notebook compute	Read			
GetNotebookExport	Grants permission to get notebook exports	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProject	Grants permission to get Project details	Read			
GetProjectProfile	Grants permission to get project profile details	Read			
GetRule	Grants permission to get rule	Read			
GetSubscription	Grants permission to retrieve a subscription	Read			
GetSubscriptionEligibility [permission only]	Grants permission to get subscription eligibilty	Read			
GetSubscriptionGrant	Grants permission to retireve a subscription grant	Read			
GetSubscriptionRequestDetails	Grants permission to reject a subscription request for a Data Asset	Read			
GetSubscriptionTarget	Grants permission to retireve details of subscription target	Read			
GetTimeSeriesDataPoint	Grants permission to get an existing TimeSeriesDataPoints in Amazon DataZone using its identifier	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUpdateEligibility	Grants permission to get update eligibility status for project constructs	Read			
GetUserProfile	Grants permission to retrieve a user profile for an existing user in the DataZone Domain	Read			
ListAccountEnvironments	Grants permission to list Environments across all domains in an AWS Account	List			
ListAccountPools	Grants permission to list account pools	List			
ListAccountsInAccountPool	Grants permission to list accounts in an account pool	List			
ListAssetFilters	Grants permission to list asset filters	List			
ListAssetRevisions	Grants permission to list revisions of an asset	List			
ListCellRuns	Grants permission to list cell runs	List			
ListConnections	Grants permission to list connections	List			
ListConversations	Grants permission to list conversations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataProductRevisions	Grants permission to list data product revisions	List			
ListDataSourceRunActivities	Grants permission to list DataSource runs job's activities on Asset	List			
ListDataSourceRuns	Grants permission to list DataSource runs job	List			
ListDataSources	Grants permission to list existing DataSources	List			
ListDomainUnitsForParent	Grants permission to list child domain units for a given parent domain unit	List			
ListDomains	Grants permission to retrieve all domains	List			
ListEntityOwners	Grants permission to list owners of an entity like domain unit	List			
ListEnvironmentActions	Grants permission to list environment actions in a default service blueprint environment	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEnvironmentBlueprintConfigurationSummaries [permission only]	Grants permission to list environment blueprint configuration summaries	List			
ListEnvironmentBlueprintConfigurations	Grants permission to list environment blueprint configurations	List			
ListEnvironmentBlueprints	Grants permission to list Domain for Environment Blueprints	List			
ListEnvironmentProfiles	Grants permission to list Domain for Environment Profiles	List			
ListEnvironments	Grants permission to show Environments in the Domain	List			
ListGroupsForUser	Grants permission to list all the DataZone group profiles that the DataZone user profile is a member of	List			
ListJobRuns	Grants permission to list job runs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLineageEvents	Grants permission to list lineage events	List			
ListLineageNodeHistory	Grants permission to list historical versions of lineage node	List			
ListLinkedTypes [permission only]	Grants permission to list linked type items linked to an Amazon DataZone Domain	List	domain*		
ListMetadataGenerationRuns	Grants permission to list metadata generation runs	List			
ListNotebooks	Grants permission to list notebooks	List			
ListNotifications	Grants permission to list notifications and events for a datazone user	List			
ListPolicyGrants	Grants permission to list policy grants	List			
ListProjectMemberships	Grants permission to list Project Members	List			
ListProjectProfiles	Grants permission to list project profiles	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProjects	Grants permission to list Projects	List			
ListRules	Grants permission to list rules	List			
ListSubscriptionGrants	Grants permission to List subscription grants for a subscribed principal	List			
ListSubscriptionRequests	Grants permission to list subscription requests	List			
ListSubscriptionTargets	Grants permission to list subscription targets	List			
ListSubscriptions	Grants permission to list subscriptions	List			
ListTagsForResource	Grants permission to retrieve all tags associated with a resource	Read	domain		
ListTimeSeriesDataPoints	Grants permission to list existing TimeSeriesDataPoints	List			
ListWarehouseMetadata [permission only]	Grants permission to list available Manager Secrets	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PostLineageEvent	Grants permission to post lineage events	Write			
PostTimeSeriesDataPoints	Grants permission to post a new TimeSeriesDataPoints	Write			
ProvisionDomain [permission only]	Grants permission to provision domain with default project setup	Write			
PutCellRunResult	Grants permission to put cell run results	Write			
PutDataExportConfiguration	Grants permission to create and update DataZone catalog data export configuration	Write			
PutDomainSharingPolicy [permission only]	Grants permission to add a resource policy for a DataZone Domain	Permissions management			
PutEnvironmentBlueprintConfiguration	Grants permission to put environment blueprint configuration	Write			
QueryGraph	Grants permission to query graph	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RefreshToken [permission only]	Grants permission to refresh token	Write			
RejectPredictions	Grants permission to reject prediction	Write			
RejectSubscriptionRequest	Grants permission to reject a subscription request for a Data Asset	Write			
RemoveEntityOwner	Grants permission to remove an existing owner of an entity like domain unit	Write			
RemovePolicyGrant	Grants permission to remove a policy grant	Permissions management			
RevokeSubscription	Grants permission to revoke a subscription	Permissions management			
Search	Grants permission to search datazone entities	List			
SearchGroupProfiles	Grants permission to search DataZone group profiles and IAM Identity Center groups	List			
SearchListings	Grants permission to search listings	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchRules [permission only]	Grants permission to search rules	List			
SearchTypes	Grants permission to search types such asset types and form types in a domain	List			
SearchUserProfiles	Grants permission to search DataZone user profiles, IAM Identity Center users, and DataZone IAM principal profiles	List			
SendMessage	Grants permission to send messages	Write			
SsoLogin [permission only]	Grants permission to login using SSO	Write			
SsoLogout [permission only]	Grants permission to logout as SSO user	Write			
StartAccountBootstrapAction [permission only]	Grants permission to start account bootstrap action for a domain	Write			
StartConversation	Grants permission to start conversations	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDataSourceRun	Grants permission to start a DataSource run job	Write			
StartMetadataGenerationRun	Grants permission to start metadata generation run	Write			
StartNotebookCompute	Grants permission to start notebook compute	Write			
StartNotebookExport	Grants permission to export notebooks	Write			
StartNotebookImport	Grants permission to import notebooks	Write			
StopMetadataGenerationRun	Grants permission to stop metadata generation run	Write			
StopNotebookCompute	Grants permission to stop notebook compute	Write			
TagResource	Grants permission to add or update tags to a resource	Tagging	domain*		
				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	domain*		
				aws:TagKeys	
UpdateAccountPool	Grants permission to update an account pool	Write			
UpdateAssetFilter	Grants permission to update asset filter	Write			
UpdateCell	Grants permission to update cells	Write			
UpdateCellRun	Grants permission to update cell runs	Write			
UpdateConnection	Grants permission to update connections	Write			
UpdateDataSource	Grants permission to update existing DataSource	Write			
UpdateDataSourceRunActivities [permission only]	Grants permission to update data source run activities	Write			
UpdateDomain	Grants permission to update information for a domain	Write	domain*		
UpdateDomainUnit	Grants permission to update an existing domain unit	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update Environment settings	Write			
UpdateEnvironmentAction	Grants permission to update an environment action in a default service blueprint environment	Write			
UpdateEnvironmentBlueprint	Grants permission to update Environment Blueprint settings	Write			
UpdateEnvironmentConfiguration [permission only]	Grants permission to update environment configuration	Write			
UpdateEnvironmentDeploymentStatus [permission only]	Grants permission to update status of the Environment deployment	Write			
UpdateEnvironmentProfile	Grants permission to update EnvironmentProfile configuration	Write			
UpdateGlossary	Grants permission to update a business glossary	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGlossaryTerm	Grants permission to update a glossary term	Write			
UpdateGroupProfile	Grants permission to update a DataZone group profile	Write			
UpdateNotebook	Grants permission to update notebooks	Write			
UpdateProject	Grants permission to update a Project that enables your team to publish and subscribe to data	Write			
UpdateProjectProfile	Grants permission to update a project profile	Write			
UpdateRule	Grants permission to update rule	Write			
UpdateSubscriptionGrantStatus	Grants permission to update a subscription grant status for custom grants	Write			
UpdateSubscriptionRequest	Grants permission to update business reason for subscription request for a Data Asset	Write			
UpdateSubscriptionTarget	Grants permission to update a subscription target	Write			
UpdateUserProfile	Grants permission to update a DataZone user profile	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidatePassRole [permission only]	Grants permission to validate pass role	Write			

Resource types defined by Amazon DataZone

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:${Partition}:datazone:${Region}:${Account}:domain/${DomainId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon DataZone

Amazon DataZone defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
datazone:domainId	Filters access by the domain ID passed in the request	String
datazone:projectId	Filters access by the project ID passed in the request	String
datazone:userId	Filters access by the user ID passed in the request	String

Actions, resources, and condition keys for AWS Deadline Cloud

AWS Deadline Cloud (service prefix: `deadline`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Deadline Cloud
- Resource types defined by AWS Deadline Cloud
- Condition keys for AWS Deadline Cloud

Actions defined by AWS Deadline Cloud

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateMemberToFarm	Grants permission to associate a member to a farm	Permissions management	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToFleet	Grants permission to associate a member to a fleet	Permissions management	fleet*		identitystore:DescribeGroup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToJob	Grants permission to associate a member to a job	Permissions management	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	
AssociateMemberToQueue	Grants permission to associate a member to a queue	Permissions management	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel deadline:MembershipLevel	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeFleetRoleForRead	Grants permission to assume a fleet role for read-only access	Write	fleet*		identitystore:ListGroupMembershipsForMember
AssumeFleetRoleForWorker	Grants permission to assume a fleet role for a worker	Write	worker*		
AssumeQueueRoleForRead	Grants permission to assume a queue role for read-only access	Write	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForUser	Grants permission to assume a queue role for a user	Write	queue*		identitystore:ListGroupMembershipsForMember
AssumeQueueRoleForWorker	Grants permission to assume a queue role for a worker	Write	queue* worker*		
BatchGetJobEntity	Grants permission to get a job entity for a worker	Read	worker*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyJobTemplate	Grants permission to copy a job template to an Amazon S3 bucket	Write	job*		identitystore:ListGroupMembershipsForMember s3:PutObject
CreateBudget	Grants permission to create a budget	Write	budget*		deadline:TagResource identitystore:ListGroupMembershipsForMember
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFarm	Grants permission to create a farm	Write	farm*		deadline:TagResource

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
CreateFleet	Grants permission to create a fleet	Write	fleet*		deadline:TagResource ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Grants permission to create a job	Write	job*		deadline:GetJobTemplate identitystore:ListGroupMembershipsForMember
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLicenseEndpoint	Grants permission to create a license endpoint for licensed software or products	Write	license-endpoint*		deadline:TagResource ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLimit	Grants permission to create a limit for a farm	Write	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMonitor	Grants permission to create a monitor	Write	monitor*		deadline:TagResource iam:PassRole sso:CreateApplication sso:DeleteApplication sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Grants permission to create a queue	Write	queue*		deadline:TagResource iam:PassRole identitystore:ListGroupMembershipsForMember logs:CreateLogGroup s3:ListBucket

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueueEnvironment	Grants permission to create a queue environment	Write	queue*		identitystore:ListGroupMembershipsForMember
CreateQueueFleetAssociation	Grants permission to create a queue-fleet association	Write	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
CreateQueueLimitAssociation	Grants permission to create a queue-limit association	Write	farm*		identitystore:ListGroupMembershipsForMember
			queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStorageProfile	Grants permission to create a storage profile for a farm	Write	farm*		identitystore:ListGroupMembershipsForMember
CreateWorker	Grants permission to create a worker	Write	worker*		deadline:ListTagsForResource deadline:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBudget	Grants permission to delete a budget	Write	budget*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFarm	Grants permission to delete a farm	Write	farm*		identitystore:ListGroupMembershipsForMember
DeleteFleet	Grants permission to delete a fleet	Write	fleet*		identitystore:ListGroupMembershipsForMember
DeleteLicenseEndpoint	Grants permission to delete a license endpoint	Write	license-endpoint*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteLimit	Grants permission to delete a limit	Write	farm*		identitystore:ListGroupMembershipsForMember
DeleteMeteredProduct	Grants permission to delete a metered product	Write	license-endpoint*		
DeleteMonitor	Grants permission to delete a monitor	Write	monitor*		sso:DeleteApplication

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteQueue	Grants permission to delete a queue	Write	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueEnvironment	Grants permission to delete a queue environment	Write	queue*		identitystore:ListGroupMembershipsForMember
DeleteQueueFleetAssociation	Grants permission to delete a queue-fleet association	Write	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteQueueLimitAssociation	Grants permission to delete a queue-limit association	Write	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
DeleteStorageProfile	Grants permission to delete a storage profile	Write	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWorker	Grants permission to delete a worker	Write	worker*		
DisassociateMemberFromFarm	Grants permission to disassociate a member from a farm	Permissions management	farm*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromFleet	Grants permission to disassociate a member from a fleet	Permissions management	fleet*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromJob	Grants permission to disassociate a member from a job	Permissions management	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				deadline:AssociatedMembershipLevel	
DisassociateMemberFromQueue	Grants permission to disassociate a member from a queue	Permissions management	queue*		identitystore:ListGroupMembershipsForMember
				deadline:AssociatedMembershipLevel	
GetApplicationVersion [permission only]	Grants permission to get the latest version of an application	Read	monitor*		
GetBudget	Grants permission to get a budget	Read	budget*		identitystore:ListGroupMembershipsForMember
GetFarm	Grants permission to get a farm	Read	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFleet	Grants permission to get a fleet	Read	fleet*		identitystore:ListGroupMembershipsForMember
GetJob	Grants permission to get a job	Read	job*		identitystore:ListGroupMembershipsForMember
GetJobTemplate [permission only]	Grants permission to read job template	Read	job*		
GetLicenseEndpoint	Grants permission to get a license endpoint	Read	license-endpoint*		
GetLimit	Grants permission to get a limit	Read	farm*		identitystore:ListGroupMembershipsForMember
GetMonitor	Grants permission to get a monitor	Read	monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQueue	Grants permission to get a queue	Read	queue*		identitystore:ListGroupMembershipsForMember
GetQueueEnvironment	Grants permission to get a queue environment	Read	queue*		identitystore:ListGroupMembershipsForMember
GetQueueFleetAssociation	Grants permission to get a queue-fleet association	Read	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
GetQueueLimitAssociation	Grants permission to get a queue-limit association	Read	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
GetSession	Grants permission to get a session for a job	Read	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSessionAction	Grants permission to get a session action for a job	Read	job*		identitystore:ListGroupMembershipsForMember
GetSessionsStatisticsAggregation	Grants permission to get all collected statistics for sessions	Read	farm*		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		
GetStep	Grants permission to get a step in a job	Read	job*		identitystore:ListGroupMembershipsForMember
GetStorageProfile	Grants permission to get a storage profile	Read	farm*		identitystore:ListGroupMembershipsForMember
GetStorageProfileForQueue	Grants permission to get a storage profile for a queue	Read	queue*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTask	Grants permission to get a job task	Read	job*		identitystore:ListGroupMembershipsForMember
GetWorker	Grants permission to get a worker	Read	worker*		identitystore:ListGroupMembershipsForMember
ListAvailableMeteredProducts	Grants permission to list all available metered products within a license endpoint	List			
ListBudgets	Grants permission to list all budgets for a farm	List	budget		identitystore:ListGroupMembershipsForMember
ListFarmMembers	Grants permission to list all members of a farm	List	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFarms	Grants permission to list all farms	List	farm*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListFleetMembers	Grants permission to list all members of a fleet	List	fleet*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFleets	Grants permission to list all fleets	List	fleet*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListJobMembers	Grants permission to list all members of a job	List	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListJobParameterDefinitions	Grants permission to get a job's parameter definitions in the job template	List	job*		identitystore:ListGroupMembershipsForMember
ListJobs	Grants permission to list all jobs in a queue	List	job*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListLicenseEndpoints	Grants permission to list all license endpoints	List	license-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLimits	Grants permission to list all limits in a farm	List	farm*		identitystore:ListGroupMembershipsForMember
ListMeteredProducts	Grants permission to list all metered products in a license endpoint	List	license-endpoint*		
ListMonitors	Grants permission to list all monitors	List	monitor*		
ListQueueEnvironments	Grants permission to list all queue environments to which a queue is associated	List	queue*		identitystore:ListGroupMembershipsForMember
ListQueueFleetAssociations	Grants permission to list all queue-fleet associations	List	farm*		identitystore:ListGroupMembershipsForMember
			fleet		
			queue		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListQueueLimitAssociations	Grants permission to list all queue-limit associations	List	farm*		identitystore:ListGroupMembershipsForMember
			queue		
ListQueueMembers	Grants permission to list all members in a queue	List	queue		identitystore:ListGroupMembershipsForMember
ListQueues	Grants permission to list all queues on a farm	List	queue*		identitystore:DescribeGroup identitystore:DescribeUser identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				deadline:PrincipalId deadline:RequesterPrincipalId	
ListSessionActions	Grants permission to list all session actions for a job	List	job*		identitystore:ListGroupMembershipsForMember
ListSessions	Grants permission to list all sessions for a job	List	job*		identitystore:ListGroupMembershipsForMember
ListSessionsForWorker	Grants permission to list all sessions for a worker	List	worker		identitystore:ListGroupMembershipsForMember
ListStepConsumers	Grants permission to list the step consumers for a job step	List	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStepDependencies	Grants permission to list dependencies for a job step	List	job		identitystore:ListGroupMembershipsForMember
ListSteps	Grants permission to list all steps for a job	List	job*		identitystore:ListGroupMembershipsForMember
ListStorageProfiles	Grants permission to list all storage profiles in a farm	List	farm*		identitystore:ListGroupMembershipsForMember
ListStorageProfilesForQueue	Grants permission to list all storage profiles in a queue	List	queue		identitystore:ListGroupMembershipsForMember
ListTagsForResource	Grants permission to list all tags on specified Deadline Cloud resources	Read	budget		
			farm		
			fleet		
			job		
			license-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			monitor		
			queue		
			worker		
				deadline:CalledAction	
ListTasks	Grants permission to list all tasks for a job	List	job*		identitystore:ListGroupMembershipsForMember
ListWorkers	Grants permission to list all workers in a fleet	List	worker*		identitystore:ListGroupMembershipsForMember
PutMeteredProduct	Grants permission to add a metered product to a license endpoint	Write	license-endpoint*		
SearchJobs	Grants permission to search for jobs in multiple queues	Read	queue*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchSteps	Grants permission to search the steps within a single job or to search the steps for multiple queues	Read	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchTasks	Grants permission to search the tasks within a single job or to search the tasks for multiple queues	Read	job		identitystore:ListGroupMembershipsForMember
			queue		
SearchWorkers	Grants permission to search for workers in multiple fleets	Read			identitystore:ListGroupMembershipsForMember
StartSessionsStatisticsAggregation	Grants permission to get all collected statistics for sessions	Read	fleet		identitystore:ListGroupMembershipsForMember
			queue		
TagResource	Grants permission to add or overwrite one or more tags for the specified Deadline Cloud resource	Tagging	budget		
			farm		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet		
			job		
			license-endpoint		
			monitor		
			queue		
			worker		
				aws:RequestTag/${TagKey} aws:TagKeys deadline:CalledAction	
UntagResource	Grants permission to disassociate one or more tags from the specified Deadline Cloud resource	Tagging	budget		
			farm		
			fleet		
			job		
			license-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			monitor		
			queue		
			worker		
				aws:TagKeys	
UpdateBudget	Grants permission to update a budget	Write	budget*		identitystore:ListGroupMembershipsForMember
UpdateFarm	Grants permission to update a farm	Write	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFleet	Grants permission to update a fleet	Write	fleet*		ec2:CreateVpcEndpoint iam:PassRole identitystore:ListGroupMembershipsForMember vpc-lattice:GetResourceConfiguration vpc-lattice:GetResourceGateway
UpdateJob	Grants permission to update a job	Write	job*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLimit	Grants permission to update a limit for a farm	Write	farm*		identitystore:ListGroupMembershipsForMember
UpdateMonitor	Grants permission to update a monitor	Write	monitor*		iam:PassRole sso:PutApplicationGrant sso:UpdateApplication
UpdateQueue	Grants permission to update a queue	Write	queue*		iam:PassRole identitystore:ListGroupMembershipsForMember
UpdateQueueEnvironment	Grants permission to update a queue environment	Write	queue*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateQueueFleetAssociation	Grants permission to update a queue-fleet association	Write	fleet*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateQueueLimitAssociation	Grants permission to update a queue-limit association	Write	farm*		identitystore:ListGroupMembershipsForMember
			queue*		
UpdateSession	Grants permission to update a session for a job	Write	job*		identitystore:ListGroupMembershipsForMember
UpdateStep	Grants permission to update a step for a job	Write	job*		identitystore:ListGroupMembershipsForMember
UpdateStorageProfile	Grants permission to update a storage profile for a farm	Write	farm*		identitystore:ListGroupMembershipsForMember

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTask	Grants permission to update a task	Write	job*		identitystore:ListGroupMembershipsForMember
UpdateWorker	Grants permission to update a worker	Write	worker*		logs:CreateLogStream
UpdateWorkerSchedule	Grants permission to update the schedule for a worker	Write	worker*		logs:CreateLogStream

Resource types defined by AWS Deadline Cloud

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:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/budget/${BudgetId}`	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels

Resource types	ARN	Condition keys
farm	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels
fleet	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels
job	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}/job/${JobId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:JobMembershipLevels deadline:QueueMembershipLevels
license-endpoint	arn:${Partition}:deadline:${Region}:${Account}:license-endpoint/${LicenseEndpointId}	aws:ResourceTag/${TagKey}
monitor	arn:${Partition}:deadline:${Region}:${Account}:monitor/${MonitorId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
queue	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/queue/${QueueId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:QueueMembershipLevels
worker	arn:${Partition}:deadline:${Region}:${Account}:farm/${FarmId}/fleet/${FleetId}/worker/${WorkerId}	aws:ResourceTag/${TagKey} deadline:FarmMembershipLevels deadline:FleetMembershipLevels

Condition keys for AWS Deadline Cloud

AWS Deadline Cloud defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
deadline:AssociatedMembershipLevel	Filters access by the associated membership level of the principal provided in the request	String
deadline:CalledAction	Filters access by the allowed action in the request	String
deadline:FarmMembershipLevels	Filters access by membership levels on the farm	ArrayOfString
deadline:FleetMembershipLevels	Filters access by membership levels on the fleet	ArrayOfString
deadline:JobMembershipLevels	Filters access by membership levels on the job	ArrayOfString
deadline:MembershipLevel	Filters access by the membership level passed in the request	String
deadline:PrincipalId	Filters access by the principle ID provided in the request	String
deadline:QueueMembershipLevels	Filters access by membership levels on the queue	ArrayOfString

Condition keys	Description	Type
deadline: RequesterPrincipalId	Filters access by the user calling the Deadline Cloud API	String

Actions, resources, and condition keys for Amazon Detective

Amazon Detective (service prefix: `detective`) 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 Detective
- Resource types defined by Amazon Detective
- Condition keys for Amazon Detective

Actions defined by Amazon Detective

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptInvitation	Grants permission to accept an invitation to become a member of a behavior graph	Write	Graph*		
BatchGetGraphMemberDatasources	Grants permission to retrieve the datasource package history for the specified member accounts in a behavior graph managed by this account	Read	Graph*		
BatchGetMembershipDatasources	Grants permission to retrieve the datasource package history of the caller account for the specified graphs	Read			
CreateGraph	Grants permission to create a behavior graph and begin to aggregate security information	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	detective:TagResource
CreateMembers	Grants permission to request the membership of one or more accounts in a behavior	Write	Graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	graph managed by this account				
DeleteGraph	Grants permission to delete a behavior graph and stop aggregating security information	Write	Graph*		
DeleteMembers	Grants permission to remove member accounts from a behavior graph managed by this account	Write	Graph*		
DescribeOrganizationConfiguration	Grants permission to view the current configuration related to the Amazon Detective integration with AWS Organizations	Read	Graph*		organizations:DescribeOrganization
DisableOrganizationAdminAccount	Grants permission to remove the Amazon Detective delegated administrator account for an organization	Write			organizations:DescribeOrganization
DisassociateMembership	Grants permission to remove the association of this account with a behavior graph	Write	Graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOrganizationAdminAccount	Grants permission to designate the Amazon Detective delegated administrator account for an organization	Write			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
GetFreeTrialEligibility [permission only]	Grants permission to retrieve a behavior graph's eligibility for a free trial period	Read	Graph*		
GetGraphIngestState [permission only]	Grants permission to retrieve the data ingestion state of a behavior graph	Read	Graph*		
GetInvestigation	Grants permission to get an investigation's status and metadata	Read	Graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMembers	Grants permission to retrieve details on specified members of a behavior graph	Read	Graph*		
GetPricingInformation [permission only]	Grants permission to retrieve information about Amazon Detective's pricing	Read			
GetUsageInformation [permission only]	Grants permission to list usage information of a behavior graph	Read	Graph*		
InvokeAssistant [permission only]	Grants permission to invoke Detective's Assistant	Read	Graph*		
ListDatasourcePackages	Grants permission to list a graph's datasource package ingest states and timestamps for the most recent state changes in a behavior graph managed by this account	List	Graph*		
ListGraphs	Grants permission to list behavior graphs managed by this account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHighDegreeEntities [permission only]	Grants permission to retrieve high volume entities whose relationships cannot be stored by Detective	List	Graph*		
ListIndicators	Grants permission to list the indicators of an investigation	List	Graph*		
ListInvestigations	Grants permission to list the investigations of a behavior graph	List	Graph*		
ListInvitations	Grants permission to retrieve details on the behavior graphs to which this account has been invited to join	List			
ListMembers	Grants permission to retrieve details on all members of a behavior graph	List	Graph*		
ListOrganizationAdminAccount	Grants permission to view the current Amazon Detective delegated administrator account for an organization	List			organizations:DescribeOrganization
ListTagsForResource	Grants permission to list the tag values that are assigned to a behavior graph	List	Graph*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectInvitation	Grants permission to reject an invitation to become a member of a behavior graph	Write	Graph*		
SearchGraph [permission only]	Grants permission to search the data stored in a behavior graph	Read	Graph*		
StartInvestigation	Grants permission to start investigations	Write	Graph*		
StartMonitoringMember	Grants permission to start data ingest for a member account that has a status of ACCEPTED_BUT_DISABLED	Write	Graph*		
TagResource	Grants permission to assign tag values to a behavior graph	Tagging	Graph*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tag values from a behavior graph	Tagging	Graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateDatasourcePackages	Grants permission to enable or disable datasource package(s) in a behavior graph managed by this account	Write	Graph*		
UpdateInvestigationState	Grants permission to update an investigation's state and metadata	Write	Graph*		
UpdateOrganizationConfiguration	Grants permission to update the current configuration related to the Amazon Detective integration with AWS Organizations	Write	Graph*		organizations:DescribeOrganization

Resource types defined by Amazon Detective

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
Graph	`arn:${Partition}:detective:${Region}:${Account}:graph:${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Detective

Amazon Detective defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by specifying the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by specifying the tags associated with the resource	String
aws:TagKeys	Filters access by specifying the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Device Farm

AWS Device Farm (service prefix: `devicefarm`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Device Farm
- Resource types defined by AWS Device Farm
- Condition keys for AWS Device Farm

Actions defined by AWS Device Farm

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDevicePool	Grants permission to create a device pool within a project	Write	project*		
CreateInstanceProfile	Grants permission to create a device instance profile	Write			
CreateNetworkProfile	Grants permission to create a network profile within a project	Write	project*		
CreateProject	Grants permission to create a project for mobile testing	Write			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRemoteAccessSession	Grants permission to start a remote access session to a device instance	Write	device*		
			project*		
			deviceinstance		
			upload		
CreateTestGridProject	Grants permission to create a project for desktop testing	Write			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
CreateTestGridUrl	Grants permission to generate a new pre-signed url used to access our test grid service	Write	testgrid-project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUpload	Grants permission to upload a new file or app within a project	Write	project*		
CreateVPCEConfiguration	Grants permission to create an Amazon Virtual Private Cloud (VPC) endpoint configuration	Write			
DeleteDevicePool	Grants permission to delete a user-generated device pool	Write	devicepool*		
DeleteInstanceProfile	Grants permission to delete a user-generated instance profile	Write	instanceprofile*		
DeleteNetworkProfile	Grants permission to delete a user-generated network profile	Write	networkprofile*		
DeleteProject	Grants permission to delete a mobile testing project	Write	project*		
DeleteRemoteAccessSession	Grants permission to delete a completed remote access session and its results	Write	session*		
DeleteRun	Grants permission to delete a run	Write	run*		
DeleteTestGridProject	Grants permission to delete a desktop testing project	Write	testgrid-project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUpload	Grants permission to delete a user-uploaded file	Write	upload*		
DeleteVPCEConfiguration	Grants permission to delete an Amazon Virtual Private Cloud (VPC) endpoint configuration	Write	vpceconfiguration*		
GetAccountSettings	Grants permission to retrieve the number of unmetered iOS and/or unmetered Android devices purchased by the account	Read			
GetDevice	Grants permission to retrieve the information of a unique device type	Read	device*		
GetDeviceInstance	Grants permission to retireve the information of a device instance	Read	deviceinstance*		
GetDevicePool	Grants permission to retireve the information of a device pool	Read	devicepool*		
GetDevicePoolCompatibility	Grants permission to retrieve information about the compatibility of a test and/or app with a device pool	Read	devicepool*		
			upload		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceProfile	Grants permission to retrieve the information of an instance profile	Read	instanceprofile*		
GetJob	Grants permission to retrieve the information of a job	Read	job*		
GetNetworkProfile	Grants permission to retrieve the information of a network profile	Read	networkprofile*		
GetOfferingStatus	Grants permission to retrieve the current status and future status of all offerings purchased by an AWS account	Read			
GetProject	Grants permission to retrieve information about a mobile testing project	Read	project*		
GetRemoteAccessSession	Grants permission to retrieve the link to a currently running remote access session	Read	session*		
GetRun	Grants permission to retrieve the information of a run	Read	run*		
GetSuite	Grants permission to retrieve the information of a testing suite	Read	suite*		
GetTest	Grants permission to retrieve the information of a test case	Read	test*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTestGridProject	Grants permission to retrieve information about a desktop testing project	Read	testgrid-project*		
GetTestGridSession	Grants permission to retireve the information of a test grid session	Read	testgrid-project		
			testgrid-session		
GetUpload	Grants permission to retireve the information of an uploaded file	Read	upload*		
GetVPCEConfiguration	Grants permission to retireve the information of an Amazon Virtual Private Cloud (VPC) endpoint configuration	Read	vpceconfiguration*		
InstallToRemoteAccessSession	Grants permission to install an application to a device in a remote access session	Write	session*		
			upload*		
ListArtifacts	Grants permission to list the artifacts in a project	List	job		
			run		
			suite		
			test		
ListDeviceInstances	Grants permission to list the information of device instances	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDevicePools	Grants permission to list the information of device pools	List	project*		
ListDevices	Grants permission to list the information of unique device types	List			
ListInstanceProfiles	Grants permission to list the information of device instance profiles	List			
ListJobs	Grants permission to list the information of jobs within a run	List	run*		
ListNetworkProfiles	Grants permission to list the information of network profiles within a project	List	project*		
ListOfferingPromotions	Grants permission to list the offering promotions	List			
ListOfferingTransactions	Grants permission to list all of the historical purchases, renewals, and system renewal transactions for an AWS account	List			
ListOfferings	Grants permission to list the products or offerings that the user can manage through the API	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProjects	Grants permission to list the information of mobile testing projects for an AWS account	List			
ListRemoteAccessSessions	Grants permission to list the information of currently running remote access sessions	List	project*		
ListRuns	Grants permission to list the information of runs within a project	List	project*		
ListSamples	Grants permission to list the information of samples within a project	List	job*		
ListSuites	Grants permission to list the information of testing suites within a job	List	job*		
ListTagsForResource	Grants permission to list the tags of a resource	List	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
ListTestGridProjects	Grants permission to list the information of desktop testing projects for an AWS account	List			
ListTestGridSessionActions	Grants permission to list the session actions performed during a test grid session	List	testgrid-session*		
ListTestGridSessionArtifacts	Grants permission to list the artifacts generated by a test grid session	List	testgrid-session*		
ListTestGridSessions	Grants permission to list the sessions within a test grid project	List	testgrid-project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTests	Grants permission to list the information of tests within a testing suite	List	suite*		
ListUniqueProblems	Grants permission to list the information of unique problems within a run	List	run*		
ListUploads	Grants permission to list the information of uploads within a project	List	project*		
ListVPCEConfigurations	Grants permission to list the information of Amazon Virtual Private Cloud (VPC) endpoint configurations	List			
PurchaseOffering	Grants permission to purchase offerings for an AWS account	Write			
RenewOffering	Grants permission to set the quantity of devices to renew for an offering	Write			
ScheduleRun	Grants permission to schedule a run	Write	project*		
			devicepool		
			upload		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: Device Pool as filter		devicepool* project* upload		
	SCENARIO: Device Selection Configuration as filter		project* upload		
StopJob	Grants permission to terminate a running job	Write	job*		
StopRemoteAccessSession	Grants permission to terminate a running remote access session	Write	session*		
StopRun	Grants permission to terminate a running test run	Write	run*		
TagResource	Grants permission to add tags to a resource	Tagging	device		
			deviceinstance		
			devicepool		
			instanceprofile		
			networkprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	device		
			deviceinstance		
			devicepool		
			instanceprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			networkprofile		
			project		
			run		
			session		
			testgrid-project		
			testgrid-session		
			vpceconfiguration		
				aws:TagKeys	
UpdateDeviceInstance	Grants permission to modify an existing device instance	Write	deviceinstance*		
			instanceprofile		
UpdateDevicePool	Grants permission to modify an existing device pool	Write	devicepool*		
UpdateInstanceProfile	Grants permission to modify an existing instance profile	Write	instanceprofile*		
UpdateNetworkProfile	Grants permission to modify an existing network profile	Write	networkprofile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProject	Grants permission to modify an existing mobile testing project	Write	project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTestGridProject	Grants permission to modify an existing desktop testing project	Write	testgrid-project*		ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:CreateServiceLinkedRole
UpdateUpload	Grants permission to modify an existing upload	Write	upload*		
UpdateVPCEConfiguration	Grants permission to modify an existing Amazon Virtual Private Cloud (VPC) endpoint configuration	Write	vpceconfiguration*		

Resource types defined by AWS Device Farm

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:${Partition}:devicefarm:${Region}:${Account}:project:${ResourceId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:devicefarm:${Region}:${Account}:run:${ResourceId}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:devicefarm:${Region}:${Account}:job:${ResourceId}	
suite	arn:${Partition}:devicefarm:${Region}:${Account}:suite:${ResourceId}	
test	arn:${Partition}:devicefarm:${Region}:${Account}:test:${ResourceId}	
upload	arn:${Partition}:devicefarm:${Region}:${Account}:upload:${ResourceId}	
artifact	arn:${Partition}:devicefarm:${Region}:${Account}:artifact:${ResourceId}	
sample	arn:${Partition}:devicefarm:${Region}:${Account}:sample:${ResourceId}	
networkprofile	arn:${Partition}:devicefarm:${Region}:${Account}:networkprofile:${ResourceId}	aws:ResourceTag/${TagKey}
deviceinstance	arn:${Partition}:devicefarm:${Region}::deviceinstance:${ResourceId}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:devicefarm:${Region}:${Account}:session:${ResourceId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
devicepool	arn:${Partition}:devicefarm:${Region}:${Account}:devicepool:${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:devicefarm:${Region}::device:${ResourceId}	aws:ResourceTag/${TagKey}
instanceprofile	arn:${Partition}:devicefarm:${Region}:${Account}:instanceprofile:${ResourceId}	aws:ResourceTag/${TagKey}
vpceconfiguration	arn:${Partition}:devicefarm:${Region}:${Account}:vpceconfiguration:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-project	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-project:${ResourceId}	aws:ResourceTag/${TagKey}
testgrid-session	arn:${Partition}:devicefarm:${Region}:${Account}:testgrid-session:${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Device Farm

AWS Device Farm defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value 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 AWS DevOps Agent Service

AWS DevOps Agent Service (service prefix: `aidevops`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS DevOps Agent Service
- Resource types defined by AWS DevOps Agent Service
- Condition keys for AWS DevOps Agent Service

Actions defined by AWS DevOps Agent Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to authorize vended logs	Permissions management			
AssociateService	Grants permission to associate service	Write	agentspace*		
			associations*		
CreateAgentSpace	Grants permission to create agentspace	Write	agentspace*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateBacklogTask	Grants permission to create a new backlog task	Write	agentspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateChat	Grants permission to create a chat	Write	agentspace*		
CreateKnowledgeItem	Grants permission to create a new knowledge item	Write	agentspace*		
DeleteAgentSpace	Grants permission to delete agentspace	Write	agentspace*		
				aws:ResourceTag/${TagKey}	
DeleteKnowledgeItem	Grants permission to delete a knowledge item	Write	agentspace*		
DeregisterService	Grants permission to deregister a service	Write	service*		
				aws:ResourceTag/${TagKey}	
DescribeSupportLevel	Grants permission to describe a chat for a case	Write	agentspace*		
DisableOperatorApp	Grants permission to disable the Operator App access to the given AgentSpace	Write	agentspace*		
DisassociateService	Grants permission to disassociate service	Write	agentspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			associations*		
DiscoverTopology	Grants permission to discover topology information	Write	agentspace*		
EnableOperatorApp	Grants permission to enable the Operator App to access the given AgentSpace	Write	agentspace*		
EndChatForCase	Grants permission to end a chat for a case	Write	agentspace*		
GetAccountUsage	Grants permission to retrieve account usage information	Read			
GetAgentSpace	Grants permission to get agentspace	Read	agentspace*		
				aws:ResourceTag/${TagKey}	
GetAssociation	Grants permission to get association	Read	agentspace*		
			associations*		
GetBacklogTask	Grants permission to get a backlog task	Read	agentspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetKnowledgeItem	Grants permission to get a knowledge item	Read	agentspace*		
GetOperatorApp	Grants permission to get operator auth config for any enabled auth flow	Read	agentspace*		
GetRecommendation	Grants permission to get a recommendation	Read	agentspace*		
GetService	Grants permission to get services	Read	service*		
				aws:ResourceTag/${TagKey}	
InitiateChatForCase	Grants permission to initiate a chat for a case	Write	agentspace*		
ListAgentSpaces	Grants permission to list agentspace	List			
ListAssociations	Grants permission to list associations	List	agentspace*		
ListBacklogTasks	Grants permission to list backlog tasks	List	agentspace*		
ListChats	Grants permission to list chats	List	agentspace*		
ListExecutions	Grants permission to list executions	List	agentspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGoals	Grants permission to list goals	List	agentspace*		
ListJournalRecords	Grants permission to list journal records	List	agentspace*		
ListKnowledgeItemVersions	Grants permission to list knowledge item versions	List	agentspace*		
ListKnowledgeItems	Grants permission to list knowledge items	List	agentspace*		
ListPendingMessages	Grants permission to list pending messages	List	agentspace*		
ListRecommendations	Grants permission to list recommendations	List	agentspace*		
ListServices	Grants permission to list services	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	agentspace	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey}	
ListWebhooks	Grants permission to list webhooks for association	List	agentspace*		
			associations*		
RegisterService	Grants permission to register specific service	Write	service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
SearchServiceAccessibleResource	Grants permission to look up a registered service accessible resources	Read			
SendMessage	Grants permission to send chat messages	Write	agentspace*		
TagResource	Grants permission to tag a resource	Tagging	agentspace	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	agentspace	aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service	aws:ResourceTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAgentSpace	Grants permission to update agentspace	Write	agentspace*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	Grants permission to update association	Write	agentspace*		
			associations*		
UpdateBacklogTask	Grants permission to update a task	Write	agentspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGoal	Grants permission to update a goal	Write	agentspace*		
UpdateKnowledgeItem	Grants permission to update a knowledge item	Write	agentspace*		
UpdateOperatorAppIdpConfig	Grants permission to update the external Identity Provider configuration for the Operator App	Write	agentspace*		
UpdateRecommendation	Grants permission to update a recommendation	Write	agentspace*		
ValidateAwsAssociations	Grants permission to validate aws association	Write	agentspace*		

Resource types defined by AWS DevOps Agent 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
agentspace	arn:${Partition}:aidevops:${Region}:${Account}:agentspace/${AgentSpaceId}	aws:ResourceTag/${TagKey}
associations	arn:${Partition}:aidevops:${Region}:${Account}:agentspace/${AgentSpaceId}/associations/${AssociationId}	
service	arn:${Partition}:aidevops:${Region}:${Account}:service/${ServiceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS DevOps Agent Service

AWS DevOps Agent Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon DevOps Guru

Amazon DevOps Guru (service prefix: `devops-guru`) 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 DevOps Guru

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddNotificationChannel	Grants permission to add a notification channel to DevOps Guru	Write	topic*		sns:GetTopicAttributes sns:SetTopicAttributes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInsight	Grants permission to delete specified insight in your account	Write			
DescribeAccountHealth	Grants permission to view the health of operations in your AWS account	Read			
DescribeAccountOverview	Grants permission to view the health of operations within a time range in your AWS account	Read			
DescribeAnomaly	Grants permission to list the details of a specified anomaly	Read			
DescribeEventSourcesConfig	Grants permission to retrieve details about event sources for DevOps Guru	Read			
DescribeFeedback	Grants permission to view the feedback details of a specified insight	Read			
DescribeInsight	Grants permission to list the details of a specified insight	Read			
DescribeOrganizationHealth	Grants permission to view the health of operations in your organization	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrganizationOverview	Grants permission to view the health of operations within a time range in your organization	Read			
DescribeOrganizationResourceCollectionHealth	Grants permission to view the health of operations for each AWS CloudFormation stack or AWS Services or accounts specified in DevOps Guru in your organization	Read			
DescribeResourceCollectionHealth	Grants permission to view the health of operations for each AWS CloudFormation stack specified in DevOps Guru	Read			
DescribeServiceIntegration	Grants permission to view the integration status of services that can be integrated with DevOps Guru	Read			
GetCostEstimation	Grants permission to list service resource cost estimates	Read			
GetResourceCollection	Grants permission to list AWS CloudFormation stacks that DevOps Guru is configured to use	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAnomaliesForInsight	Grants permission to list anomalies of a given insight in your account	List		devops-guru:ServiceNames	
ListAnomalousLogGroups	Grants permission to list log anomalies of a given insight in your account	List			
ListEvents	Grants permission to list resource events that are evaluated by DevOps Guru	List			
ListInsights	Grants permission to list insights in your account	List			
ListMonitoredResources	Grants permission to list resource monitored by DevOps Guru in your account	List			
ListNotificationChannels	Grants permission to list notification channels configured for DevOps Guru in your account	List			
ListOrganizationInsights	Grants permission to list insights in your organization	List			
ListRecommendations	Grants permission to list a specified insight's recommendations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFeedback	Grants permission to submit a feedback to DevOps Guru	Write			
RemoveNotificationChannel	Grants permission to remove a notification channel from DevOps Guru	Write	topic*		sns:GetTopicAttributes sns:SetTopicAttributes
SearchInsights	Grants permission to search insights in your account	List		devops-guru:ServiceNames	
SearchOrganizationInsights	Grants permission to search insights in your organization	List			
StartCostEstimation	Grants permission to start the creation of an estimate of the monthly cost	Read			
UpdateEventSourcesConfig	Grants permission to update an event source for DevOps Guru	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResourceCollection	Grants permission to update the list of AWS CloudFormation stacks that are used to specify which AWS resources in your account are analyzed by DevOps Guru	Write			
UpdateServiceIntegration	Grants permission to enable or disable a service that integrates with DevOps Guru	Write			

Resource types defined by Amazon DevOps Guru

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}`	

Condition keys for Amazon DevOps Guru

Amazon DevOps Guru defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
devops-guru:ServiceNames	Filters access by API to restrict access to given AWS service names	ArrayOfString

Actions, resources, and condition keys for AWS Diagnostic tools

AWS Diagnostic tools (service prefix: `ts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Diagnostic tools
- Resource types defined by AWS Diagnostic tools
- Condition keys for AWS Diagnostic tools

Actions defined by AWS Diagnostic tools

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExecution	Grants permission to get details about specific	Read	execution *		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	execution within AWS Diagnostic tools				
GetExecutionOutput	Grants permission to get details about specific execution output within AWS Diagnostic tools	Read	execution*		
GetTool	Grants permission to get details about specific tool within AWS Diagnostic tools	Read	tool*		
ListExecutions	Grants permission to list all available execution within AWS Diagnostic tools	List			
ListTagsForResource	Grants permission to list the tags for an AWS Diagnostic tools resource	Read	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListTools	Grants permission to list all available tools within AWS Diagnostic tools	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartExecution	Grants permission to start an execution workflow of specific tool within AWS Diagnostic tools	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
TagResource	Grants permission to tag an AWS Diagnostic tools resource	Tagging	execution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag an AWS Diagnostic tools resource	Tagging	execution*		
				aws:TagKeys	

Resource types defined by AWS Diagnostic tools

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
execution	arn:${Partition}:ts::${Account}:execution/${UserId}/${ToolId}/${ExecutionId}	aws:ResourceTag/${TagKey}
tool	arn:${Partition}:ts::aws:tool/${ToolId}	

Condition keys for AWS Diagnostic tools

AWS Diagnostic tools defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Direct Connect

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDirectConnectGatewayAssociationProposal	Grants permission to accept a proposal request to attach a virtual private gateway to a Direct Connect gateway	Write	dx-gateway*		
AllocateConnectionOnInterconnect	Grants permission to create a hosted connection on an interconnect	Write	dxcon*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateHostedConnection	Grants permission to create a new hosted connection between a AWS Direct Connect partner's network and a specific AWS 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		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
AssociateMacSecKey	Grants permission to associate a MAC Security (MACsec) Connection Key Name (CKN)/ Connectivity Association Key (CAK) pair with an AWS 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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnection	Grants permission to create a new connection between the customer network and a specific AWS 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	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInterconnect	Grants permission to create a new interconnect between a AWS Direct Connect partner's network and a specific AWS Direct Connect location	Write	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLag	Grants permission to create a link aggregation group (LAG) with the specified number of bundled physical connections between the customer network and a specific AWS Direct Connect location	Write	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateVirtualInterface	Grants permission to create a new private virtual interface	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	Grants permission to create a new public virtual interface	Write	dxcon		
			dxlag		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	Grants permission to create a new transit virtual interface	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account	Read	dxcon		
DescribeLags	Grants permission to describe all your link aggregation groups (LAG) or the specified LAG	Read	dxlag		
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 AWS Direct Connect locations in the current AWS region	Read			
DescribeRouterConfiguration	Grants permission to describe Details about the router for a virtual interface	Read	dxvif*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTags	Grants permission to describe the tags associated with the specified AWS Direct Connect resources	Read	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
DescribeVirtualGateways	Grants permission to describe a list of virtual private gateways owned by the AWS account	Read			
DescribeVirtualInterfaces	Grants permission to describe all virtual interfaces for an AWS account	Read	dxcon		
			dxlag		
			dxvif		
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 AWS Direct Connect dedicated connection	Write	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	Grants permission to list the virtual interface failover test history	List	dxvif*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Direct Connect resource. Each resource can have a maximum of 50 tags	Tagging	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from the specified AWS Direct Connect resource	Tagging	dx-gateway		
			dxcon		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dxlag		
			dxvif		
				aws:TagKeys	
UpdateConnection	Grants permission to update the AWS 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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVirtualInterfaceAttributes	Grants permission to update the specified attributes of the specified virtual private interface	Write	dxvif*		

Resource types defined by AWS 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/${TagKey}
dxlag	`arn:${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 AWS Direct Connect

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Directory Service

AWS 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 AWS Directory Service
- Resource types defined by AWS Directory Service
- Condition keys for AWS Directory Service

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 ec2:AuthorizeSecurityGroupIngress ec2:DescribeSecurityGroups
AddRegion	Grants permission to add two domain controllers in	Write	directory*		ec2:AuthorizeSecur

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	the specified Region for the specified directory				ityGroupEgress 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 AWS 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 AWS 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
CreateHybridAD	Grants permission to create a Hybrid Managed AD directory	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeVpcs iam:CreateServiceLinkedRole iam:GetRole secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIdentityPoolDirectory [permission only]	Grants permission to create an IdentityPool Directory in the AWS 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 AWS account	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMicrosoftAD	Grants permission to create a Microsoft AD in the AWS 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 AWS cloud	Write	directory*		
CreateTrust	Grants permission to initiate the creation of the AWS side of a trust relationship between a Microsoft AD in the AWS cloud and an external domain	Write	directory*		
DeleteADAssessment	Grants permission to delete a directory assessment	Write			
DeleteConditionalForwarder	Grants permission to delete a conditional forwarder that has been set up for your AWS directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDirectory	Grants permission to delete an AWS 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 AWS 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*		
DescribeADAssessment	Grants permission to describe a directory assessment	Read			
DescribeCAEnrollmentPolicy	Grants permission to describe the ca enrollment status of a specified directory	Read	directory*		
DescribeCertificate	Grants permission to display information about the certificate registered for a secured LDAP connection	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEventTopics	Grants permission to obtain information about which SNS topics receive status messages from the specified directory	Read	directory*		
DescribeHybridADUpdate	Grants permission to describe the updates of a specified hybrid directory	Read	directory*		
DescribeLDAPSSettings	Grants permission to describe the status of LDAP security for the specified directory	Read	directory*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DisableCAEnrollmentPolicy	Grants permission to disable the ca enrollment of a specified directory	Write	directory*		
DisableClientAuthentication	Grants permission to disable alternative client authentication methods for the specified directory	Write	directory*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableRoleAccess [permission only]	Grants permission to disable AWS Management Console access for identity in your AWS Directory	Write	directory*		
DisableSso	Grants permission to disable single-sign on for a directory	Write	directory*		
EnableCAEnrollmentPolicy	Grants permission to enable the ca enrollment of a specified directory	Write	directory*		acm-pca:DescribeCertificateAuthority pca-connector-ad:GetConnector
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*		
EnableLDAPS	Grants permission to activate the switch for the specific directory to always use LDAP secure calls	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Management Console access for identity in your AWS 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			
GetSnapshotLimits	Grants permission to obtain the manual snapshot limits for a directory	Read	directory*		
ListADAssessments	Grants permission to list directory assessments	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAuthorizedApplications [permission only]	Grants permission to obtain the AWS 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 AWS 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*		
RegisterCertificate	Grants permission to register a certificate for secured LDAP connection	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetUserPassword	Grants permission to reset the password for any user in your AWS 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 AWS account (directory owner) with another AWS account (directory consumer). With this operation you can use your directory from any AWS account and from any Amazon VPC within an AWS Region	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartADAssessment	Grants permission to start a directory assessment	Write			ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetwor

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kInterfaces ec2:DescribeSubnets ec2:DescribeVpcs ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand
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 AWS Directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Directory	Write	directory*		
UpdateConditionalForwarder	Grants permission to update a conditional forwarder that has been set up for your AWS 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*		
UpdateDirectorySetup	Grants permission to update the directory for a particular update type	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateHybridAD	Grants permission to update configurations for a specified hybrid directory	Write	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeVpcs secretsmanager:DescribeSecret secretsmanager:GetSecretValue ssm:GetCommandInvocation ssm:GetConnectionStatus ssm:ListCommands ssm:SendCommand

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateTrust	Grants permission to update the trust that has been set up between your AWS Managed Microsoft AD directory and an on-premises Active Directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
VerifyTrust	Grants permission to verify a trust relationship between your Microsoft AD in the AWS cloud and an external domain	Read	directory *		

Resource types defined by AWS 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 AWS Directory Service

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the value of the request to AWS DS	String
aws:ResourceTag/${TagKey}	Filters access by the AWS 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 AWS Directory Service Data

AWS Directory Service Data (service prefix: `ds-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 AWS Directory Service Data
- Resource types defined by AWS Directory Service Data
- Condition keys for AWS Directory Service Data

Actions defined by AWS Directory Service Data

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddGroupMember	Grants permission to add a member to a group on a directory	Write	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:MemberName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
CreateGroup	Grants permission to create a group on a directory	Write	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser	Grants permission to create a user on a directory	Write	directory *		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteGroup	Grants permission to delete a group on a directory	Write	directory *		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DeleteUser	Grants permission to delete a user on a directory	Write	directory *		ds:AccessDSData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeGroup	Grants permission to describe a group on a directory	Read	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DescribeUser	Grants permission to describe a user on a directory	Read	directory*		ds:AccessDSData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
DisableUser	Grants permission to disable a user on a directory	Write	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
ListGroupMembers	Grants permission to list members in a group on a directory	List	directory*		ds:AccessDSData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListGroups	Grants permission to list groups on a directory	List	directory*		ds:AccessDSData
				ds-data:Realm	
ListGroupsForMember	Grants permission to list the groups that a member is in on a directory	List	directory*		ds:AccessDSData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ds-data:SAMAccountName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
ListUsers	Grants permission to list users on a directory	List	directory*		ds:AccessDSData
				ds-data:Realm	
RemoveGroupMember	Grants permission to remove a member from a group on a directory	Write	directory*		ds:AccessDSData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ds-data:SAMAccountName ds-data:MemberName ds-data:Realm ds-data:MemberRealm ds-data:Identifier	
SearchGroups	Grants permission to search for groups on a directory	Read	directory*		ds-data:DescribeGroup ds:AccessDSData
				ds-data:Realm	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchUsers	Grants permission to search for users on a directory	Read	directory*		ds-data:DescribeUser ds:AccessDSData
				ds-data:Realm	
UpdateGroup	Grants permission to update a group on a directory	Write	directory*		ds:AccessDSData
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	
UpdateUser	Grants permission to update a user on a directory	Write	directory*		ds:AccessDSData

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ds-data:SAMAccountName ds-data:Identifier ds-data:Realm	

Resource types defined by AWS Directory Service Data

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 AWS Directory Service Data

AWS Directory Service Data defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the AWS DS Resource being acted upon	String
ds-data:Identifier	Filters access by the type of identifier provided in the request (i.e. SAM Account Name)	String
ds-data:MemberName	Filters access by the directory SAM Account Name included in the MemberName input of the request	String
ds-data:MemberRealm	Filters access by the directory realm name included in the MemberRealm input of the request	String
ds-data:Realm	Filters access by the directory realm name for the request	String
ds-data:SAMAccountName	Filters access by the directory SAM Account Name included in the SAMAccountName input of the request	String

Actions, resources, and condition keys for Amazon DocumentDB Elastic Clusters

Amazon DocumentDB Elastic Clusters (service prefix: `docdb-elastic`) 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 DocumentDB Elastic Clusters

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApplyPendingMaintenanceAction	Grants permission to apply pending maintenance actions on Amazon DocDB-Elastic cluster	Write	cluster*		
				aws:ResourceTag/${TagKey}	
CopyClusterSnapshot	Grants permission to copy a new Amazon DocDB-Elastic cluster snapshot	Write	cluster-snapshot*		docdb-elastic:CreateClusterSnapshot kms:CreateGrant kms:Decrypt kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:GenerateDataKey
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a new Amazon DocDB-Elastic cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClusterSnapshot	Grants permission to create a new Amazon DocDB-Elastic cluster snapshot	Write	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:Get

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					SecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCluster	Grants permission to delete a cluster	Write	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClusterSnapshot	Grants permission to delete a cluster snapshot	Write	cluster-snapshot*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetCluster	Grants permission to view details about a cluster	Read	cluster*		
				aws:ResourceTag/${TagKey}	
GetClusterSnapshot	Grants permission to view details about a cluster snapshot	Read	cluster-snapshot*		
				aws:ResourceTag/${TagKey}	
GetPendingMaintenanceAction	Grants permission to view details about pending maintenance actions on Amazon DocDB-Elastic cluster	Read	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusterSnapshots	Grants permission to list the cluster snapshots in your account	List			
ListClusters	Grants permission to list the clusters in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPendingMaintenanceActions	Grants permission to list details about pending maintenance actions on any Amazon DocDB-Elastic cluster	List		aws:ResourceTag/${TagKey}	
ListTagsForResource	Grants permission to lists tag for an DocumentDB Elastic resource	List	cluster		
			cluster-snapshot		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreClusterFromSnapshot	Grants permission to restore cluster from a Amazon DocDB-Elastic cluster snapshot	Write	cluster*		docdb-elastic:CreateCluster ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeVpcs ec2:ModifyVpcEndpoint iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:GetSecretValue secretsmanager:ListSecretVersionIds secretsmanager:ListSecrets
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
StartCluster	Grants permission to start a stopped Amazon DocDB-Elastic cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
StopCluster	Grants permission to stop an existing Amazon DocDB-Elastic cluster	Write	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag an DocumentDB Elastic resource	Tagging	cluster		
			cluster-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a DocumentDB Elastic resource	Tagging	cluster		
			cluster-snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	Grants permission to modify a cluster	Write	cluster*		ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:ModifyVpcEndpoint kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey secretsmanager:DescribeSecret secretsmanager:GetResourcePolicy secretsmanager:GetSecretValue secretsmanager:Lis

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					tSecretVersionIds secretsmanager:ListSecrets
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon DocumentDB Elastic 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:${Partition}:docdb-elastic:${Region}:${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
cluster-snapshot	`arn:${Partition}:docdb-elastic:${Region}:${Account}:cluster-snapshot/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon DocumentDB Elastic Clusters

Amazon DocumentDB Elastic Clusters defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws: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

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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTableReplica [permission only]	Grants permission to create multi account global table replica	Write	table*		
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			table*		
CreateGlobalTableWitness [permission only]	Grants permission to add a Witness to a Global Table	Write	table*		
CreateTable	Grants permission to the CreateTable operation adds a new table to your account	Write	table*		
				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*		
DeleteGlobalTableWitness [permission only]	Grants permission to remove a Witness from a Global Table	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteItem	Grants permission to deletes a single item in a table by primary key	Write	table*		
				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 AWS 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*		
InjectError [permission only]	Grants permission to start experiments on a Global Table	Write		dynamodb:FisActionId dynamodb:FisTargetArns	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
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	
ReadDataForReplication [permission only]	Grants permission to read data from a multi account global table replica	Read	table*		
ReplicateSettings [permission only]	Grants permission to configure settings for a multi account global table replica	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreTableFromAwsBackup [permission only]	Grants permission to create a new table from recovery point on AWS Backup	Write	table*		
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 AWS 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*		
WriteDataForReplication [permission only]	Grants permission to write data to a multi account global table replica	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}
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 AWS 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:FirstPartitionKeyValues	Filters access by the first partition key of the table	ArrayOfString
dynamodb:FisActionId	Filters access by the ID of an AWS FIS action	String
dynamodb:FisTargetArns	Filters access by the ARN of an AWS FIS target	ArrayOfARN

Condition keys	Description	Type
dynamodb:FourthPartitionKeyValues	Filters access by the forth partition key of the table	ArrayOfString
dynamodb:FullTableScan	Filters access by blocking full table scan	Bool
dynamodb:LeadingKeys	Filters access by the first partition key of the table	ArrayOfString
dynamodb:ReturnConsumedCapacity	Filters access by the ReturnConsumedCapacity parameter of a request. Contains either "TOTAL" or "NONE"	String
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:SecondPartitionKeyValues	Filters access by the second partition key of the table	ArrayOfString
dynamodb:Select	Filters access by the Select parameter of a Query or Scan request	String
dynamodb:ThirdPartitionKeyValues	Filters access by the third partition key of the table	ArrayOfString

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)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetItem	Grants permission to return the attributes of one or more items from one or more tables	Read	application*		
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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAddressTransfer	Grants permission to accept an Elastic IP address transfer	Write	elastic-ip*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Domain ec2:PublicIpAddress	ec2:CreateTags
				ec2:Region	
AcceptCapacityReservationBillingOwnership	Grants permission to accept assign billing of the available capacity of a shared Capacity Reservation to the calling account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptReservedInstancesExchangeQuote	Grants permission to accept a Convertible Reserved Instance exchange quote	Write	reserved-instances*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptTransitGatewayMulticastDomainAssociations	Grants permission to accept a request to associate subnets with a transit gateway multicast domain	Write	transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptTransitGatewayPeeringAttachment	Grants permission to accept a transit gateway peering attachment request	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
AcceptTransitGatewayVpcAttachment	Grants permission to accept a request to attach a VPC to a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AcceptVpcEndpointConnections	Grants permission to accept one or more interface VPC endpoint connections to your VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptVpcPeeringConnection	Grants permission to accept a VPC peering connection request	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AdvertiseByoipCidr	Grants permission to advertise an IP address range that is provisioned for use in AWS through bring your own IP addresses (BYOIP)	Write		ec2:Region	
AllocateAddress	Grants permission to allocate an Elastic IP address (EIP) to your account	Write	elastic-ip*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateHosts	Grants permission to allocate a Dedicated Host to your account	Write	dedicated-host*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:Quantity	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateIpamPoolCidr	Grants permission to allocate a CIDR from an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApplySecurityGroupsToClientVpnTargetNetwork	Grants permission to apply a security group to the association between a Client VPN endpoint and a target network	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignIpv6Addresses	Grants permission to assign one or more IPv6 addresses to a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignPrivateIpAddresses	Grants permission to assign one or more secondary private IP addresses to a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignPrivateNatGatewayAddress	Grants permission to assign one or more secondary private IP addresses to a private NAT gateway	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateAddress	Grants permission to associate an Elastic IP address (EIP) with an instance or a network interface	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateCapacityReservationBillingOwner	Grants permission to assign billing of the unused capacity of a shared Capacity Reservation to a consumer account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateClientVpnTargetNetwork	Grants permission to associate a target network with a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
AssociateDhcpOptions	Grants permission to associate or disassociate a set of DHCP options with a VPC	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
AssociateEnclaveCertificateIamRole	Grants permission to associate an ACM certificate with an IAM role to be used in an EC2 Enclave	Write	certificate*		
			role*		
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateIamInstanceProfile	Grants permission to associate an IAM instance profile with a running or stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
AssociateInstanceEventWindow	Grants permission to associate one or more targets with an event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AssociateIpamByoasn	Grants permission to associate an Autonomous System Number (ASN) with a BYOIP CIDR	Write		ec2:Region	
AssociateIpamResourceDiscovery	Grants permission to associate an IPAM resource discovery with an Amazon VPC IPAM	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery-association*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
AssociateNatGatewayAddress	Grants permission to associate an Elastic IP address and private IP address with a public Nat gateway	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateRouteServer	Grants permission to associate a route server with a VPC	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate RouteTable	Grants permission to associate a subnet or gateway with a route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateSecurityGroupVpc	Grants permission to associate a security group with another VPC in the same Region	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateSubnetCidrBlock	Grants permission to associate a CIDR block with a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTransitGatewayMulticastDomain	Grants permission to associate an attachment and list of subnets with a transit gateway multicast domain	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTransitGatewayPolicyTable	Grants permission to associate a policy table with a transit gateway attachment	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTransitGatewayRouteTable	Grants permission to associate an attachment with a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTrunkInterface	Grants permission to associate a branch network interface with a trunk network interface	Write		ec2:Region	
AssociateVerifiedAccessInstanceWebAcl [permission only]	Grants permission to associate an AWS Web Application Firewall (WAF) web access control list (ACL) with a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate VpcCidrBlock	Grants permission to associate a CIDR block with a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AttachAppliance ToNatGateway [permission only]	Grants permission to attach an appliance with a public/private Natgateway	Permissions management	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachClassicLinkVpc	Grants permission to link an EC2-Classic instance to a ClassicLink-enabled VPC through one or more of the VPC's security groups	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
AttachInternetGateway	Grants permission to attach an internet gateway to a VPC	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachNetworkInterface	Grants permission to attach a network interface to an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachResourcesToPlacementGroup [permission only]	Grants permission to attach resources to a placement group	Permissions management	placement-group*	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	
AttachVerifiedAccessTrustProvider	Grants permission to attach a trust provider to 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
			verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachVolume	Grants permission to attach an EBS volume to a running or stopped instance and expose it to the instance with the specified device name	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachVpnGateway	Grants permission to attach a virtual private gateway to a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeClientVpnIngress	Grants permission to add an inbound authorization rule to a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AuthorizeSecurityGroupEgress	Grants permission to add one or more outbound rules to a VPC security group. Policies using the security-group-rule resource-level permission are only enforced when the API request includes TagSpecifications	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	ec2:CreateTags
			security-group-rule	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeSecurityGroupIngress	Grants permission to add one or more inbound rules to a VPC security group. Policies using the security-group-rule resource-level permission are only enforced when the API request includes TagSpecifications	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	ec2:CreateTags
			security-group-rule	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
BundleInstance	Grants permission to bundle an instance store-backed Windows instance	Write		ec2:Region	
CancelBundleTask	Grants permission to cancel a bundling operation	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelCapacityReservation	Grants permission to cancel a Capacity Reservation and release the reserved capacity	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
CancelCapacityReservationFleets	Grants permission to cancel one or more Capacity Reservation Fleets	Write	capacity-reservation-fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CancelCapacityReservation
				ec2:Region	
CancelConversionTask	Grants permission to cancel an active conversion task	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelDeclarativePoliciesReport	Grants permission to cancel a declarative policies report	Write	declarative-policies-report*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelExportTask	Grants permission to cancel an active export task	Write	export-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			export-instance-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CancelImageLaunchPermission	Grants permission to remove your AWS account from the launch permissions for the specified AMI	Permissions management	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelImportTask	Grants permission to cancel an in-process import virtual machine or import snapshot task	Write	import-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			import-snapshot-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelReservedInstancesListing	Grants permission to cancel a Reserved Instance listing on the Reserved Instance Marketplace	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelSpotFleetRequests	Grants permission to cancel one or more Spot Fleet requests	Write	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelSpotInstanceRequests	Grants permission to cancel one or more Spot Instance requests	Write	spot-instances-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ConfirmProductInstance	Grants permission to determine whether an owned product code is associated with an instance	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyFpgaImage	Grants permission to copy a source Amazon FPGA image (AFI) to the current Region. Resource-level permissions specified for this action apply to the new AFI only. They do not apply to the source AFI	Write	fpga-image*	ec2:Owner	
				ec2:Region	
CopyImage	Grants permission to copy an Amazon Machine Image (AMI) from a source Region to the current Region	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopySnapshot	Grants permission to copy a point-in-time snapshot of an EBS volume and store it in Amazon S3. Resource-level permissions specified for this action apply to both the snapshot copy and the source snapshot	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Encrypted ec2:OutpostArn ec2:Owner ec2:ParentSnapshot ec2:ParentVolume ec2:ProductCode ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyVolumes	Grants permission to create a copy of an EBS volume. Resource-level permissions specified for this action apply to the source and copied volume. Condition keys for the copied volume correspond to parameters specified in the CopyVolumes API request	Write	volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:VolumeInitializationRate	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
CreateCapacityManagerDataExport	Grants permission to create a new S3 Data Export for Capacity Manager	Write	capacity-manager-data-export*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservation	Grants permission to create a Capacity Reservation	Write	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CapacityReservationFleet ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:EphemeralStorage	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceCount ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservationBySplitting	Grants permission to create a new Capacity Reservation by splitting the available capacity of the source Capacity Reservation	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservationFleet	Grants permission to create a Capacity Reservation Fleet	Write	capacity-reservation-fleet*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateCapacityReservation ec2:CreateTags ec2:DescribeCapacityReservations ec2:DescribeInstances
				ec2:Region	
CreateCarrierGateway	Grants permission to create a carrier gateway and provides CSP connectivity to VPC customers	Write	carrier-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClientVpnEndpoint	Grants permission to create a Client VPN endpoint	Write	client-vpn-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:SamlProviderArn ec2:ServerCertificateArn	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClientVpnRoute	Grants permission to add a network route to a Client VPN endpoint's route table	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
CreateCoipCidr	Grants permission to create a range of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCoipPool	Grants permission to create a pool of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateCoipPoolPermission [permission only]	Grants permission to allow a service to access a customer-owned IP (CoIP) pool	Permissions management	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomerGateway	Grants permission to create a customer gateway, which provides information to AWS about your customer gateway device	Write	customer-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateDefaultSubnet	Grants permission to create a default subnet in a specified Availability Zone in a default VPC	Write		ec2:Region	
CreateDefaultVpc	Grants permission to create a default VPC with a default subnet in each Availability Zone	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDelegateMacVolumeOwnershipTask	Grants permission to create a volume ownership delegation task for an Apple silicon Mac instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceMarketType ec2:InstanceMetadataTags	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mac-modification-task*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateDhcpOptions	Grants permission to create a set of DHCP options for a VPC	Write	dhcp-options*	aws:RequestTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID	ec2:CreateTags
				ec2:Region	
CreateEgressOnlyInternetGateway	Grants permission to create an egress-only internet gateway for a VPC	Write	egress-only-internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFleet	Grants permission to launch an EC2 Fleet. Resource-level permissions for this action do not include the resources specified in a launch template. To specify resource-level permissions for resources specified in a launch template, you must include the resources in the RunInstances action statement	Write	fleet*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			instance*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dthWeighting ec2:InstanceID ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
CreateFlowLogs	Grants permission to create one or more flow logs to capture IP traffic for a network interface	Write	vpc-flow-log*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags ecs:ListClusters ecs:ListContainerInstances ecs:ListServices ecs:ListTaskDefinitions ecs:ListTasks iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Vpc	
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFpgaImage	Grants permission to create an Amazon FPGA Image (AFI) from a design checkpoint (DCP)	Write	fpga-image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Owner ec2:Public	ec2:CreateTags
				ec2:Region	
CreateImage	Grants permission to create an Amazon EBS-backed AMI from a stopped or running Amazon EBS-backed instance. This action can reboot instances as part of the image creation process, even without RebootInstances permissions. To prevent instance reboots during image creation, use the NoReboot parameter	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImageUsageReport	Grants permission to create an AMI usage report	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateTags
			image-usage-report*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstanceConnectEndpoint	Grants permission to create an EC2 Instance Connect Endpoint that allows you to connect to an instance without a public IPv4 address	Write	instance-connect-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SubnetID	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
CreateInstanceEventWindow	Grants permission to create an event window in which scheduled events for the associated Amazon EC2 instances can run	Write	instance-event-window*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstanceExportTask	Grants permission to export a running or stopped instance to an Amazon S3 bucket	Write	export-instance-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
CreateInternetGateway	Grants permission to create an internet gateway for a VPC	Write	internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:InternetGatewayID	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInterruptibleCapacityReservationAllocation	Grants permission to create an interruptible Capacity Reservation by specifying the number of unused instances you want to allocate from your source reservation	Write	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CreateDate ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount ec2:InstanceMatchCriteria	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstancePlatform ec2:InstanceType ec2:InterruptibleCapacityReservationId ec2:InterruptionType ec2:IsInterruptible ec2:SourceCapacityReservationId ec2:TargetInstanceCount ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateIpam	Grants permission to create an Amazon VPC IP Address Manager (IPAM)	Write	ipam*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	
CreateIpamExternalResourceVerificationToken	Grants permission to create a verification token, which proves ownership of an external resource	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-external-resource-verification-token*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIpamPolicy	Grants permission to create a policy in Amazon VPC IP Address Manager (IPAM) that defines rules for allocating public IPv4 addresses from IPAM pools to AWS resources	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-policy*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateIpamPool	Grants permission to create an IP address pool for Amazon VPC IP Address Manager (IPAM), which is a collection of contiguous IP address CIDRs	Write	ipam-pool*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateIpamPrefixListResolver	Grants permission to create an IPAM prefix list resolver that defines rules for selecting CIDRs to include in prefix lists	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-prefix-list-resolver*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateIpamPrefixListResolverTarget	Grants permission to create an IPAM prefix list resolver target that links a resolver to a managed prefix list	Write	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-prefix-list-resolver-target*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIpamResourceDiscovery	Grants permission to create an IPAM resource discovery	Write	ipam-resource-discovery*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	
CreateIpamScope	Grants permission to create an Amazon VPC IP Address Manager (IPAM) scope, which is the highest-level container within IPAM	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-scope*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKeyPair	Grants permission to create a 2048-bit RSA key pair	Write	key-pair*	aws:RequestTag/${TagKey} aws:TagKeys ec2:KeyPairType	ec2:CreateTags
				ec2:Region	
CreateLaunchTemplate	Grants permission to create a launch template	Write	launch-template*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags ssm:GetParameters
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLaunchTemplateVersion	Grants permission to create a new version of a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	ssm:GetParameters
				ec2:Region	
CreateLocalGatewayRoute	Grants permission to create a static route for a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayRouteTable	Grants permission to create a local gateway route table	Write	local-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocalGatewayRouteTablePermission [permission only]	Grants permission to allow a service to access a local gateway route table	Permissions management	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayRouteTableVirtualInterfaceGroupAssociation	Grants permission to create a local gateway route table virtual interface group association	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table-virtual-interface-group-association*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayRouteTableVpcAssociation	Grants permission to associate a VPC with a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table-vpc-association*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateLocalGatewayVirtualInterface	Grants permission to create a local gateway virtual interface	Write	local-gateway-virtual-interface*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			outpost-lag*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayVirtualInterfaceGroup	Grants permission to create a local gateway virtual interface group	Write	local-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMacSystemIntegrityProtectionModificationTask	Grants permission to create a System Integrity Protection (SIP) modification task for an Amazon EC2 Mac instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceMarketType ec2:InstanceMetadataTags	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mac-modification-task*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateManagedPrefixList	Grants permission to create a managed prefix list	Write	prefix-list*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateNatGateway	Grants permission to create a NAT gateway in a subnet	Write	natgateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateNetworkAcl	Grants permission to create a network ACL in a VPC	Write	network-acl*	aws:RequestTag/${TagKey} aws:TagKeys ec2:NetworkAclID	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateNetworkAclEntry	Grants permission to create a numbered entry (a rule) in a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateNetworkInsightsAccessScope	Grants permission to create a Network Access Scope	Write	network-insights-access-scope*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateNetworkInsightsPath	Grants permission to create a path to analyze for reachability	Write	network-insights-path*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkInterface	Grants permission to create a network interface in a subnet	Write	network-interface*	aws:RequestTag/${TagKey} aws:TagKeys ec2:NetworkInterfaceID	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkInterfacePermission	Grants permission to create a permission for an AWS-authorized user to perform certain operations on a network interface	Permissions management	network-interface*	aws:ResourceTag/${TagKey} ec2:AuthorizedService ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Vpc	
				ec2:Region	
CreateOdbNetworkPeering [permission only]	Grants permission to allow Oracle Database@AWS to create a peering connection between an ODB network and a VPC	Permissions management	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePlacementGroup	Grants permission to create a placement group	Write	placement-group*	aws:RequestTag/${TagKey} aws:TagKeys ec2:PlacementGroupName ec2:PlacementGroupStrategy	ec2:CreateTags
				ec2:Region	
CreatePublicIpv4Pool	Grants permission to create a public IPv4 address pool for public IPv4 CIDRs that you own and bring to Amazon to manage with Amazon VPC IP Address Manager (IPAM)	Write	ipv4pool-ec2*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplaceRootVolumeTask	Grants permission to create a root volume replacement task	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			replace-root-volume-task*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VolumeID ec2:VolumeInitializationRate	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	
CreateReservedInstancesListing	Grants permission to create a listing for Standard Reserved Instances to be sold in the Reserved Instance Marketplace	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRestoreImageTask	Grants permission to start a task that restores an AMI from an S3 object previously created by using CreateStoreImageTask	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags
				ec2:Region	
CreateRoute	Grants permission to create a route in a VPC route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouteServer	Grants permission to create a route server	Write	route-server*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags sns:CreateTopic
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouteServerEndpoint	Grants permission to create a route server endpoint	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeSecurityGroups

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone	
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateRouteServerPeer	Grants permission to create a route server peer	Write	route-server-endpoint*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey}	ec2:AuthorizeSecurityGroupIngress ec2:CreateTags
			route-server-peer*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouteTable	Grants permission to create a route table for a VPC	Write	route-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:RouteTableID	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSecondaryNetwork	Grants permission to create a secondary network	Write	secondary-network*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateSecondarySubnet	Grants permission to create a secondary subnet	Write	secondary-network*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			secondary-subnet*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSecurityGroup	Grants permission to create a security group	Write	security-group*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SecurityGroupID	ec2:CreateTags
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshot	Grants permission to create a snapshot of an EBS volume and store it in Amazon S3	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Location ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SourceAvailabilityZone ec2:SourceOutpostArn ec2:VolumeSize	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshots	Grants permission to create crash-consistent snapshots of multiple EBS volumes and store them in Amazon S3	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Location ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SourceAvailabilityZone ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateSpotDatafeedSubscription	Grants permission to create a data feed for Spot Instances to view Spot Instance usage logs	Write		ec2:Region	
CreateStoreImageTask	Grants permission to store an AMI as a single object in an S3 bucket	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubnet	Grants permission to create a subnet in a VPC	Write	subnet*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:SubnetID	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubnetCidrReservation	Grants permission to create a subnet CIDR reservation	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTags	Grants permission to add or overwrite one or more tags for Amazon EC2 resources	Tagging	capacity-block	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-manager-data-export	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	
			capacity-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation-fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			carrier-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			client-vpn-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:SamlProviderArn ec2:ServerCertificateArn	
			coip-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			customer-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			declarative-policies-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dedicated-host	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:Quantity ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dhcp-options	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			egress-only-internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-gpu	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ElasticGpuType ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-ip	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-instance-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fpga-image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			host-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image-usage-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-snapshot-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-connect-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:SubnetID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-event-window	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-external-resource-verification-token	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-virtual-interface-group-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-vpc-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-acl	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-path	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:Subnet ec2:Vpc	
			placement-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replace-root-volume-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			reserved-instances	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-network	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-subnet	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} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-fleet-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-instances-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet-cidr-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-session	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-connect-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-metering-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-policy-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table-announcement	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-trust-provider	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-block-public-access-exclusion	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-encryption-control	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceRegion ec2:VpceSupportedRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service-permission	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-flow-log	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-concentrator	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	
				ec2:CreateAction ec2:Region	
CreateTrafficMirrorFilter	Grants permission to create a traffic mirror filter	Write	traffic-mirror-filter*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficMirrorFilterRule	Grants permission to create a traffic mirror filter rule	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			traffic-mirror-filter-rule*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficMirrorSession	Grants permission to create a traffic mirror session	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-session*	aws:RequestTag/${TagKey} aws:TagKeys	
			traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficMirrorTarget	Grants permission to create a traffic mirror target	Write	traffic-mirror-target*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			network-interface	aws:ResourceTag/${TagKey} ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceServiceName ec2:VpceServiceOwner	
				ec2:Region	
CreateTransitGateway	Grants permission to create a transit gateway	Write	transit-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateTransitGatewayConnect	Grants permission to create a Connect attachment from a specified transit gateway attachment	Write	transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	ec2:CreateTags
				ec2:Region	
CreateTransitGatewayConnectPeer	Grants permission to create a Connect peer between a transit gateway and an appliance	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-connect-peer*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayConnectPeerId	
				ec2:Region	
CreateTransitGatewayMeteringPolicy	Grants permission to create a metering policy for a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-metering-policy*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayMeteringPolicyId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayMeteringPolicyEntry	Grants permission to create an entry for a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayMulticastDomain	Grants permission to create a multicast domain for a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-multicast-domain*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayPeeringAttachment	Grants permission to request a transit gateway peering attachment between a requester and accepter transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayPolicyTable	Grants permission to create a transit gateway policy table	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-policy-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayPrefixListReference	Grants permission to create a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
CreateTransitGatewayRoute	Grants permission to create a static route for a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
CreateTransitGatewayRouteTable	Grants permission to create a route table for a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayRouteTableId	
				ec2:Region	
CreateTransitGatewayRouteTableAnnouncement	Grants permission to create an announcement for a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-route-table-announcement*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayVpcAttachment	Grants permission to attach a VPC to a transit gateway	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	ec2:CreateTags
			transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVerifiedAccessEndpoint	Grants permission to create a Verified Access endpoint	Write	verified-access-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
CreateVerifiedAccessGroup	Grants permission to create a Verified Access group	Write	verified-access-group*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVerifiedAccessInstance	Grants permission to create a Verified Access instance	Write	verified-access-instance*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateVerifiedAccessTrustProvider	Grants permission to create a verified trust provider	Write	verified-access-trust-provider*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVolume	Grants permission to create an EBS volume	Write	volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeInitializationRate	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpc	Grants permission to create a VPC with a specified CIDR block	Write	vpc*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:VpcID	ec2:CreateTags
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpcBlockPublicAccessExclusion	Grants permission to create an exclusion list for blocked public access on a VPC	Write	vpc-block-public-access-exclusion*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEncryptionControl	Grants permission to create a VPC Encryption Control	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	ec2:CreateTags
			vpc-encryption-control*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEndpoint	Grants permission to create a VPC endpoint for an AWS service	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	ec2:CreateTags ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs route53:AssociateVPCWithHostedZone

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceMultiRegion ec2:VpcePrivateDnsPreference ec2:VpcePrivateDnsSpecifiedDomains ec2:VpceServiceName ec2:VpceServiceOwner ec2:VpceServiceRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
CreateVpcEndpointConnectionNotification	Grants permission to create a connection notification for a VPC endpoint or VPC endpoint service	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEndpointServiceConfiguration	Grants permission to create a VPC endpoint service configuration to which service consumers (AWS accounts, IAM users, and IAM roles) can connect	Write	vpc-endpoint-service*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceMultiRegion ec2:VpceServicePrivateDnsName ec2:VpceServiceRegion	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcPeeringConnection	Grants permission to request a VPC peering connection between two VPCs	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	ec2:CreateTags
			vpc-peering-connection*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:RequesterVpc ec2:VpcPeeringConnectionID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateVpnConcentrator	Grants permission to create a VPN concentrator that aggregates multiple VPN connections to a transit gateway	Write	vpn-concentrator*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpnConnection	Grants permission to create a VPN connection between a virtual private gateway or transit gateway and a customer gateway	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-connection*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:RoutingType	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			vpn-concentrator	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpnConnectionRoute	Grants permission to create a static route for a VPN connection between a virtual private gateway and a customer gateway	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpnGateway	Grants permission to create a virtual private gateway	Write	vpn-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteCapacityManagerDataExport	Grants permission to delete an existing Capacity Manager data export configuration	Write	capacity-manager-data-export*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCarrierGateway	Grants permission to delete a carrier gateway	Write	carrier-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClientVpnEndpoint	Grants permission to delete a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClientVpnRoute	Grants permission to delete a route from a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCoipCidr	Grants permission to delete a range of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCoipPool	Grants permission to delete a pool of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCoipPoolPermission [permission only]	Grants permission to deny a service from accessing a customer-owned IP (CoIP) pool	Permissions management	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCustomerGateway	Grants permission to delete a customer gateway	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDhcpOptions	Grants permission to delete a set of DHCP options	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteEgressOnlyInternetGateway	Grants permission to delete an egress-only internet gateway	Write	egress-only-internet-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFleets	Grants permission to delete one or more EC2 Fleets	Write	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteFlowLogs	Grants permission to delete one or more flow logs	Write	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFpgaImage	Grants permission to delete an Amazon FPGA Image (AFI)	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteImageUsageReport	Grants permission to delete an AMI usage report	Write	image-usage-report*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInstanceConnectEndpoint	Grants permission to delete an EC2 Instance Connect Endpoint	Write	instance-connect-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
DeleteInstanceEventWindow	Grants permission to delete the specified event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInternetGateway	Grants permission to delete an internet gateway	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpam	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) and remove all monitored data associated with the IPAM including the historical data for CIDRs	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamExternalResourceVerificationToken	Grants permission to delete a verification token, which proves ownership of an external resource	Write	ipam-external-resource-verification-token*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamPolicy	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) policy	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamPool	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamPrefixListResolver	Grants permission to delete an IPAM prefix list resolver	Write	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamPrefixListResolverTarget	Grants permission to delete an IPAM prefix list resolver target	Write	ipam-prefix-list-resolver-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamResourceDiscovery	Grants permission to delete an IPAM resource discovery	Write	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamScope	Grants permission to delete the scope for an Amazon VPC IP Address Manager (IPAM)	Write	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteKeyPair	Grants permission to delete a key pair by removing the public key from Amazon EC2	Write	key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLaunchTemplate	Grants permission to delete a launch template and its associated versions	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLaunchTemplateVersions	Grants permission to delete one or more versions of a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayRoute	Grants permission to delete a route from a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRouteTable	Grants permission to delete a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteLocalGatewayRouteTablePermission [permission only]	Grants permission to deny a service from accessing a local gateway route table	Permissions management	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRouteTableVirtualInterfaceGroupAssociation	Grants permission to delete a local gateway route table virtual interface group association	Write	local-gateway-route-table-virtual-interface-group-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayRouteTableVpcAssociation	Grants permission to delete an association between a VPC and local gateway route table	Write	local-gateway-route-table-vpc-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayVirtualInterface	Grants permission to delete a local gateway virtual interface	Write	local-gateway-virtual-interface*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayVirtualInterfaceGroup	Grants permission to delete a local gateway virtual interface group	Write	local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteManagedPrefixList	Grants permission to delete a managed prefix list	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNatGateway	Grants permission to delete a NAT gateway	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkAcl	Grants permission to delete a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkAclEntry	Grants permission to delete an inbound or outbound entry (rule) from a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	
DeleteNetworkInsightsAccessScope	Grants permission to delete a Network Access Scope	Write	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInsightsAccessScopeAnalysis	Grants permission to delete a Network Access Scope analysis	Write	network-insights-access-scope-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkInsightsAnalysis	Grants permission to delete a network insights analysis	Write	network-insights-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInsightsPath	Grants permission to delete a network insights path	Write	network-insights-path*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInterface	Grants permission to delete a detached network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInterfacePermission	Grants permission to delete a permission that is associated with a network interface	Permissions management	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOdbNetworkPeering [permission only]	Grants permission to allow Oracle Database@AWS to delete a peering connection between an ODB network and a VPC	Permissions management	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePlacementGroup	Grants permission to delete a placement group	Write	placement-group*	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeletePublicIpv4Pool	Grants permission to delete a public IPv4 address pool for public IPv4 CIDRs that you own and brought to Amazon to manage with Amazon VPC IP Address Manager (IPAM)	Write	ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteQueuedReservedInstances	Grants permission to delete the queued purchases for the specified Reserved Instances	Write	reserved-instances*	aws:ResourceTag/${TagKey} ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	
DeleteResourcePolicy [permission only]	Grants permission to remove an IAM policy that enables cross-account sharing from a resource	Permissions management	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoute	Grants permission to delete a route from a route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DeleteRouteServer	Grants permission to delete a route server	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	sns:DeleteTopic
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRouteServerEndpoint	Grants permission to delete a route server endpoint	Write	route-server-endpoint*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey}	ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:RevokeSecurityGroupIngress
				ec2:Region	
DeleteRouteServerPeer	Grants permission to delete a route server peer	Write	route-server-peer*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey}	ec2:RevokeSecurityGroupIngress
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRouteTable	Grants permission to delete a route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DeleteSecondaryNetwork	Grants permission to delete a secondary network	Write	secondary-network*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSecondarySubnet	Grants permission to delete a secondary subnet	Write	secondary-subnet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
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/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${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-block	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-manager-data-export	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation-fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			carrier-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			client-vpn-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			coip-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			customer-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			declarative-policies-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dedicated-host	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dhcp-options	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			egress-only-internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-gpu	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-ip	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-instance-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fpga-image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			host-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image-usage-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-snapshot-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-connect-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-event-window	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-external-resource-verification-token	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-virtual-interface-group-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-vpc-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-acl	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-path	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replace-root-volume-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			reserved-instances	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-network	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-subnet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-fleet-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-instances-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet-cidr-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-session	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-connect-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-metering-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-policy-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table-announcement	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-trust-provider	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-block-public-access-exclusion	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-encryption-control	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service-permission	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-flow-log	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-concentrator	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	
				aws:TagKeys ec2:Region	
DeleteTrafficMirrorFilter	Grants permission to delete a traffic mirror filter	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTrafficMirrorFilterRule	Grants permission to delete a traffic mirror filter rule	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-filter-rule*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTrafficMirrorSession	Grants permission to delete a traffic mirror session	Write	traffic-mirror-session*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteTrafficMirrorTarget	Grants permission to delete a traffic mirror target	Write	traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGateway	Grants permission to delete a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
				ec2:Region	
DeleteTransitGatewayConnect	Grants permission to delete a transit gateway connect attachment	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayConnectPeer	Grants permission to delete a transit gateway connect peer	Write	transit-gateway-connect-peer*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayMeteringPolicy	Grants permission to delete a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	
				ec2:Region	
DeleteTransitGatewayMeteringPolicyEntry	Grants permission to delete an entry from a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayMulticastDomain	Grants permission to delete a transit gateway multicast domain	Write	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayPeeringAttachment	Grants permission to delete a peering attachment from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
DeleteTransitGatewayPolicyTable	Grants permission to delete a transit gateway policy table	Write	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayPrefixListReference	Grants permission to delete a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayRoute	Grants permission to delete a route from a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	
DeleteTransitGatewayRouteTable	Grants permission to delete a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayRouteTableAnnouncement	Grants permission to delete a transit gateway route table announcement	Write	transit-gateway-route-table-announcement*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayVpcAttachment	Grants permission to delete a VPC attachment from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
DeleteVerifiedAccessEndpoint	Grants permission to delete a Verified Access endpoint	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedAccessGroup	Grants permission to delete a Verified Access group	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVerifiedAccessInstance	Grants permission to delete a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedAccessTrustProvider	Grants permission to delete a verified trust provider	Write	verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVolume	Grants permission to delete an EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpc	Grants permission to delete a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DeleteVpcBlockPublicAccessExclusion	Grants permission to delete an exclusion list for blocked public access on a VPC	Write	vpc-block-public-access-exclusion*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEncryptionControl	Grants permission to delete a VPC Encryption Control	Write	vpc-encryption-control*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVpcEndpointConnectionNotifications	Grants permission to delete one or more VPC endpoint connection notifications	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEndpointServiceConfigurations	Grants permission to delete one or more VPC endpoint service configurations	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEndpoints	Grants permission to delete one or more VPC endpoints	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceName ec2:VpceServiceRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcPeeringConnection	Grants permission to delete a VPC peering connection	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	
DeleteVpnConcentrator	Grants permission to delete a VPN concentrator	Write	vpn-concentrator*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteVpnConnection	Grants permission to delete a VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVpnConnectionRoute	Grants permission to delete a static route for a VPN connection between a virtual private gateway and a customer gateway	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpnGateway	Grants permission to delete a virtual private gateway	Write	vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionByoipCidr	Grants permission to release an IP address range that was provisioned through bring your own IP addresses (BYOIP), and to delete the corresponding address pool	Write		ec2:Region	
DeprovisionIpamByoasn	Grants permission to deprovision an Autonomous System Number (ASN) from an Amazon Web Services account	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeprovisionIpamPoolCidr	Grants permission to deprovision a CIDR provisioned from an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionPublicIpv4PoolCidr	Grants permission to deprovision a CIDR from a public IPv4 pool	Write	ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterImage	Grants permission to deregister an Amazon Machine Image (AMI)	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DeregisterInstanceEventNotificationAttributes	Grants permission to remove tags from the set of tags to include in notifications about scheduled events for your instances	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterTransitGatewayMulticastGroupMembers	Grants permission to deregister one or more network interface members from a group IP address in a transit gateway multicast domain	Write	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterTransitGatewayMulticastGroupSources	Grants permission to deregister one or more network interface sources from a group IP address in a transit gateway multicast domain	Write	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	
DescribeAccountAttributes	Grants permission to describe the attributes of the AWS account	List		ec2:Region	
DescribeAddressTransfers	Grants permission to describe an Elastic IP address transfer	List		ec2:Region	
DescribeAddresses	Grants permission to describe one or more Elastic IP addresses	List		ec2:Region	
DescribeAddressesAttribute	Grants permission to describe the attributes of the specified Elastic IP addresses	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAggregateIdFormat	Grants permission to describe the longer ID format settings for all resource types	List		ec2:Region	
DescribeAvailabilityZones	Grants permission to describe one or more of the Availability Zones that are available to you	List		ec2:Region	
DescribeAwsNetworkPerformanceMetricSubscriptions	Grants permission to describe the current infrastructure performance metric subscriptions	List		ec2:Region	
DescribeBundleTasks	Grants permission to describe one or more bundling tasks	List		ec2:Region	
DescribeByoipCidrs	Grants permission to describe the IP address ranges that were provisioned through bring your own IP addresses (BYOIP)	List		ec2:Region	
DescribeCapacityBlockExtensionHistory	Grants permission to describe Capacity Block extensions history	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapacityBlockExtensionOfferings	Grants permission to describe Capacity Block extensions offerings	List	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapacityBlockOfferings	Grants permission to describe Capacity Block offerings available for purchase	List		ec2:Region	
DescribeCapacityBlockStatus	Grants permission to describe the availability of capacity for the specified Capacity blocks, or all of your Capacity Blocks	List		ec2:Region	
DescribeCapacityBlocks	Grants permission to describe details about Capacity Blocks in the AWS Region that you're currently using	List		ec2:Region	
DescribeCapacityManagerDataExports	Grants permission to describe one or more Capacity Manager data export configurations	List		ec2:Region	
DescribeCapacityReservationBillingRequests	Grants permission to describe one or more requests to assign the billing of the unused capacity of a Capacity Reservation	List		ec2:Region	
DescribeCapacityReservationFleets	Grants permission to describe one or more Capacity Reservation Fleets	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapacityReservationTopology	Grants permission to describe the topology of one or more Capacity Reservations	List		ec2:Region	
DescribeCapacityReservations	Grants permission to describe one or more Capacity Reservations	List		ec2:Region	
DescribeCarrierGateways	Grants permission to describe one or more Carrier Gateways	List		ec2:Region	
DescribeClassicLinkInstances	Grants permission to describe one or more linked EC2-Classic instances	List		ec2:Region	
DescribeClientVpnAuthorizationRules	Grants permission to describe the authorization rules for a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnConnections	Grants permission to describe active client connections and connections that have been terminated within the last 60 minutes for a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DescribeClientVpnEndpoints	Grants permission to describe one or more Client VPN endpoints	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnRoutes	Grants permission to describe the routes for a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnTargetNetworks	Grants permission to describe the target networks that are associated with a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DescribeCoipPools	Grants permission to describe the specified customer-owned address pools or all of your customer-owned address pools	List		ec2:Region	
DescribeConversionTasks	Grants permission to describe one or more conversion tasks	List		ec2:Region	
DescribeCustomerGateways	Grants permission to describe one or more customer gateways	List		ec2:Region	
DescribeDeclarativePoliciesReports	Grants permission to describe one or more declarative policies reports	List		ec2:Region	
DescribeDhcpOptions	Grants permission to describe one or more DHCP options sets	List		ec2:Region	
DescribeEgressOnlyInternetGateways	Grants permission to describe one or more egress-only internet gateways	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeElasticGpus	Grants permission to describe an Elastic Graphics accelerator that is associated with an instance	List		ec2:Region	
DescribeExportImageTasks	Grants permission to describe one or more export image tasks	List		ec2:Region	
DescribeExportTasks	Grants permission to describe one or more export instance tasks	List		ec2:Region	
DescribeFastLaunchImages	Grants permission to describe fast-launch enabled Windows AMIs	List		ec2:Region	
DescribeFastSnapshotRestores	Grants permission to describe the state of fast snapshot restores for snapshots	List		ec2:Region	
DescribeFleetHistory	Grants permission to describe the events for an EC2 Fleet during a specified time	List	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFleetInstances	Grants permission to describe the running instances for an EC2 Fleet	List	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeFleets	Grants permission to describe one or more EC2 Fleets	List		ec2:Region	
DescribeFlowLogs	Grants permission to describe one or more flow logs	List		ec2:Region	
DescribeFpgaImageAttribute	Grants permission to describe the attributes of an Amazon FPGA Image (AFI)	List	fpga-image*	aws:ResourceTag/${TagKey} ec2:Owner ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFpgaImages	Grants permission to describe one or more Amazon FPGA Images (AFIs)	List		ec2:Region	
DescribeHostReservationOfferings	Grants permission to describe the Dedicated Host Reservations that are available to purchase	List		ec2:Region	
DescribeHostReservations	Grants permission to describe the Dedicated Host Reservations that are associated with Dedicated Hosts in the AWS account	List		ec2:Region	
DescribeHosts	Grants permission to describe one or more Dedicated Hosts	List		ec2:Region	
DescribeIamInstanceProfileAssociations	Grants permission to describe the IAM instance profile associations	List		ec2:Region	
DescribeIdFormat	Grants permission to describe the ID format settings for resources	List		ec2:Region	
DescribeIdentityIdFormat	Grants permission to describe the ID format settings for resources for an IAM user, IAM role, or root user	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageAttribute	Grants permission to describe an attribute of an Amazon Machine Image (AMI)	List	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DescribeImageReferences	Grants permission to describe your AWS resources that are referencing specified images	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageUsageReportEntries	Grants permission to describe the entries of an AMI usage report	List		ec2:Region	
DescribeImageUsageReports	Grants permission to describe the configuration and status of an AMI usage report	List		ec2:Region	
DescribeImages	Grants permission to describe one or more images (AMIs, AKIs, and ARIs)	List		ec2:Region	
DescribeImportImageTasks	Grants permission to describe import virtual machine or import snapshot tasks	List		ec2:Region	
DescribeImportSnapshotTasks	Grants permission to describe import snapshot tasks	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstanceAttribute	Grants permission to describe the attributes of an instance	List	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
DescribeInstanceConnectEndpoints	Grants permission to describe EC2 Instance Connect Endpoints	List		ec2:Region	
DescribeInstanceCreditSpecifications	Grants permission to describe the credit option for CPU usage of one or more burstable performance instances	List		ec2:Region	
DescribeInstanceEventNotificationAttributes	Grants permission to describe the set of tags to include in notifications about scheduled events for your instances	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstanceEventWindows	Grants permission to describe the specified event windows or all event windows	List		ec2:Region	
DescribeInstanceImageMetadata	Grants permission to describe the AMI that was used to launch an instance	List		ec2:Region	
DescribeInstanceSqlHaHistoryStates	Grants permission to describe EC2 instance SQL HA history states	List		ec2:Region	
DescribeInstanceSqlHaStates	Grants permission to describe EC2 instance SQL HA states	List		ec2:Region	
DescribeInstanceStatus	Grants permission to describe the status of one or more instances	List		ec2:Region	
DescribeInstanceTopology	Grants permission to describe a tree-based hierarchy that represents the physical host placement of EC2 instances	List		ec2:Region	
DescribeInstanceTypeOfferings	Grants permission to describe the set of instance types that are offered in a location	List		ec2:Region	
DescribeInstanceTypes	Grants permission to describe the details of instance types that are offered in a location	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstances	Grants permission to describe one or more instances	List		ec2:Region	
DescribeInternetGateways	Grants permission to describe one or more internet gateways	List		ec2:Region	
DescribeIpamByoasn	Grants permission to describe a bring your own Autonomous System Number (BYOASN) that you've brought to IPAM	List		ec2:Region	
DescribeIpamExternalResourceVerificationTokens	Grants permission to describe verification tokens, which proves ownership of an external resource	List		ec2:Region	
DescribeIpamPolicies	Grants permission to describe Amazon VPC IP Address Manager (IPAM) policies	List		ec2:Region	
DescribeIpamPools	Grants permission to describe Amazon VPC IP Address Manager (IPAM) pools	List		ec2:Region	
DescribeIpamPrefixListResolverTargets	Grants permission to describe IPAM prefix list resolver targets	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIpamPrefixListResolvers	Grants permission to describe IPAM prefix list resolvers	List		ec2:Region	
DescribeIpamResourceDiscoveries	Grants permission to describe IPAM resource discoveries	List		ec2:Region	
DescribeIpamResourceDiscoveryAssociations	Grants permission to describe resource discovery associations with an Amazon VPC IPAM	List		ec2:Region	
DescribeIpamScopes	Grants permission to describe Amazon VPC IP Address Manager (IPAM) scopes	List		ec2:Region	
DescribeIpams	Grants permission to describe an Amazon VPC IP Address Manager (IPAM)	List		ec2:Region	
DescribeIpv6Pools	Grants permission to describe one or more IPv6 address pools	List		ec2:Region	
DescribeKeyPairs	Grants permission to describe one or more key pairs	List		ec2:Region	
DescribeLaunchTemplateVersions	Grants permission to describe one or more launch template versions	List		ec2:Region	ssm:GetParameters

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLaunchTemplates	Grants permission to describe one or more launch templates	List		ec2:Region	
DescribeLocalGatewayRouteTablePermissions [permission only]	Grants permission to allow a service to describe local gateway route table permissions	List		ec2:Region	
DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Grants permission to describe the associations between virtual interface groups and local gateway route tables	List		ec2:Region	
DescribeLocalGatewayRouteTableVpcAssociations	Grants permission to describe an association between VPCs and local gateway route tables	List		ec2:Region	
DescribeLocalGatewayRouteTables	Grants permission to describe one or more local gateway route tables	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocalGatewayVirtualInterfaceGroups	Grants permission to describe local gateway virtual interface groups	List		ec2:Region	
DescribeLocalGatewayVirtualInterfaces	Grants permission to describe local gateway virtual interfaces	List		ec2:Region	
DescribeLocalGateways	Grants permission to describe one or more local gateways	List		ec2:Region	
DescribeLockedSnapshots	Grants permission to describe the lock status for a snapshot	List		ec2:Region	
DescribeMacHosts	Grants permission to describe your EC2 Mac Dedicated hosts	List		ec2:Region	
DescribeMacModificationTasks	Grants permission to describe a System Integrity Protection (SIP) modification task or volume ownership delegation task for an Amazon EC2 Mac instance	List		ec2:Region	
DescribeManagedPrefixLists	Grants permission to describe your managed prefix lists and any AWS-managed prefix lists	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMovingAddresses	Grants permission to describe Elastic IP addresses that are being moved to the EC2-VPC platform	List		ec2:Region	
DescribeNatGateways	Grants permission to describe one or more NAT gateways	List		ec2:Region	
DescribeNetworkAcls	Grants permission to describe one or more network ACLs	List		ec2:Region	
DescribeNetworkInsightsAccessScopeAnalyses	Grants permission to describe one or more Network Access Scope analyses	List		ec2:Region	
DescribeNetworkInsightsAccessScopes	Grants permission to describe the Network Access Scopes	List		ec2:Region	
DescribeNetworkInsightsAnalyses	Grants permission to describe one or more network insights analyses	List		ec2:Region	
DescribeNetworkInsightsPaths	Grants permission to describe one or more network insights paths	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNetworkInterfaceAttribute	Grants permission to describe a network interface attribute	List		ec2:Region	
DescribeNetworkInterfacePermissions	Grants permission to describe the permissions that are associated with a network interface	List		ec2:Region	
DescribeNetworkInterfaces	Grants permission to describe one or more network interfaces	List		ec2:Region	
DescribeOutpostLags	Grants permission to describe Outpost LAGs	List		ec2:Region	
DescribePlacementGroups	Grants permission to describe one or more placement groups	List		ec2:Region	
DescribePrefixLists	Grants permission to describe available AWS services in a prefix list format	List		ec2:Region	
DescribePrincipalIdFormat	Grants permission to describe the ID format settings for the root user and all IAM roles and IAM users that have explicitly specified a longer ID (17-character ID) preference	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePublicIpv4Pools	Grants permission to describe one or more IPv4 address pools	List		ec2:Region	
DescribeRegions	Grants permission to describe one or more AWS Regions that are currently available in your account	List		ec2:Region	
DescribeReplaceRootVolumeTasks	Grants permission to describe a root volume replacement task	List		ec2:Region	
DescribeReservedInstances	Grants permission to describe one or more purchased Reserved Instances in your account	List		ec2:Region	
DescribeReservedInstancesListings	Grants permission to describe your account's Reserved Instance listings in the Reserved Instance Marketplace	List		ec2:Region	
DescribeReservedInstancesModifications	Grants permission to describe the modifications made to one or more Reserved Instances	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedInstancesOfferings	Grants permission to describe the Reserved Instance offerings that are available for purchase	List		ec2:Region	
DescribeRouteServerEndpoints	Grants permission to describe one or more route server endpoints	List		ec2:Region	
DescribeRouteServerPeers	Grants permission to describe one or more route server peers	List		ec2:Region	
DescribeRouteServers	Grants permission to describe one or more route servers	List		ec2:Region	
DescribeRouteTables	Grants permission to describe one or more route tables	List		ec2:Region	
DescribeScheduledInstanceAvailability	Grants permission to find available schedules for Scheduled Instances	List		ec2:Region	
DescribeScheduledInstances	Grants permission to describe one or more Scheduled Instances in your account	List		ec2:Region	
DescribeSecondaryInterfaces	Grants permission to describe one or more secondary interfaces	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSecondaryNetworks	Grants permission to describe one or more secondary networks	List		ec2:Region	
DescribeSecondarySubnets	Grants permission to describe one or more secondary subnets	List		ec2:Region	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
DescribeServiceLinkVirtualInterfaces	Grants permission to describe service link virtual interfaces	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSnapshotAttribute	Grants permission to describe an attribute of a snapshot	List	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DescribeSnapshotTierStatus	Grants permission to describe the storage tier status for Amazon EBS snapshots	List		ec2:Region	
DescribeSnapshots	Grants permission to describe one or more EBS snapshots	List		ec2:Region	
DescribeSpotDatafeedSubscription	Grants permission to describe the data feed for Spot Instances	List		ec2:Region	
DescribeSpotFleetInstances	Grants permission to describe the running instances for a Spot Fleet	List	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSpotFleetRequestHistory	Grants permission to describe the events for a Spot Fleet request during a specified time	List	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeSpotFleetRequests	Grants permission to describe one or more Spot Fleet requests	List		ec2:Region	
DescribeSpotInstanceRequests	Grants permission to describe one or more Spot Instance requests	List		ec2:Region	
DescribeSpotPriceHistory	Grants permission to describe the Spot Instance price history	List		ec2:Region	
DescribeStaleSecurityGroups	Grants permission to describe the stale security group rules for security groups in a specified VPC	List		ec2:Region	
DescribeStoreImageTasks	Grants permission to describe the progress of the AMI store tasks	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSubnets	Grants permission to describe one or more subnets	List		ec2:Region	
DescribeTags	Grants permission to describe one or more tags for an Amazon EC2 resource	List		ec2:Region	
DescribeTrafficMirrorFilterRules	Grants permission to describe traffic mirror filters that determine the traffic that is mirrored	List		ec2:Region	
DescribeTrafficMirrorFilters	Grants permission to describe one or more traffic mirror filters	List		ec2:Region	
DescribeTrafficMirrorSessions	Grants permission to describe one or more traffic mirror sessions	List		ec2:Region	
DescribeTrafficMirrorTargets	Grants permission to describe one or more traffic mirror targets	List		ec2:Region	
DescribeTransitGatewayAttachments	Grants permission to describe one or more attachments between resources and transit gateways	List		ec2:Region	
DescribeTransitGatewayConnectPeers	Grants permission to describe one or more transit gateway connect peers	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTransitGatewayConnects	Grants permission to describe one or more transit gateway connect attachments	List		ec2:Region	
DescribeTransitGatewayMeteringPolicies	Grants permission to describe one or more transit gateway metering policies	List		ec2:Region	
DescribeTransitGatewayMulticastDomains	Grants permission to describe one or more transit gateway multicast domains	List		ec2:Region	
DescribeTransitGatewayPeeringAttachments	Grants permission to describe one or more transit gateway peering attachments	List		ec2:Region	
DescribeTransitGatewayPolicyTables	Grants permission to describe a transit gateway policy table	List		ec2:Region	
DescribeTransitGatewayRouteTableAnnouncements	Grants permission to describe a transit gateway route table announcement	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTransitGatewayRouteTables	Grants permission to describe one or more transit gateway route tables	List		ec2:Region	
DescribeTransitGatewayVpcAttachments	Grants permission to describe one or more VPC attachments on a transit gateway	List		ec2:Region	
DescribeTransitGateways	Grants permission to describe one or more transit gateways	List		ec2:Region	
DescribeTrunkInterfaceAssociations	Grants permission to describe one or more network interface trunk associations	List		ec2:Region	
DescribeVerifiedAccessEndpoints	Grants permission to describe the specified Verified Access endpoints or all Verified Access endpoints	List		ec2:Region	
DescribeVerifiedAccessGroups	Grants permission to describe the specified Verified Access groups or all Verified Access groups	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVerifiedAccessInstanceLoggingConfigurations	Grants permission to describe the current logging configuration for the Verified Access instances	List		ec2:Region	
DescribeVerifiedAccessInstanceWebAclAssociations [permission only]	Grants permission to describe the AWS Web Application Firewall (WAF) web access control list (ACL) associations for a Verified Access instance	List		ec2:Region	
DescribeVerifiedAccessInstances	Grants permission to describe the specified Verified Access instances or all Verified Access instances	List		ec2:Region	
DescribeVerifiedAccessTrustProviders	Grants permission to describe details of existing Verified Access trust providers	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVolumeAttribute	Grants permission to describe an attribute of an EBS volume	List	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
DescribeVolumeStatus	Grants permission to describe the status of one or more EBS volumes	List		ec2:Region	
DescribeVolumes	Grants permission to describe one or more EBS volumes	List		ec2:Region	
DescribeVolumesModifications	Grants permission to describe the current modification status of one or more EBS volumes	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcAttribute	Grants permission to describe an attribute of a VPC	List	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DescribeVpcBlockPublicAccessExclusions	Grants permission to describe an exclusion list for blocked public access on a VPC	List		ec2:Region	
DescribeVpcBlockPublicAccessOptions	Grants permission to describe options for blocked public access on a VPC	List		ec2:Region	
DescribeVpcClassicLink	Grants permission to describe the ClassicLink status of one or more VPCs	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcClassicLinkDnsSupport	Grants permission to describe the ClassicLink DNS support status of one or more VPCs	List		ec2:Region	
DescribeVpcEncryptionControls	Grants permission to describe one or more VPC Encryption Controls	List		ec2:Region	
DescribeVpcEndpointAssociations	Grants permission to describe the VPC endpoint associations	List		ec2:Region	
DescribeVpcEndpointConnectionNotifications	Grants permission to describe the connection notifications for VPC endpoints and VPC endpoint services	List		ec2:Region	
DescribeVpcEndpointConnections	Grants permission to describe the VPC endpoint connections to your VPC endpoint services	List		ec2:Region	
DescribeVpcEndpointServiceConfigurations	Grants permission to describe VPC endpoint service configurations (your services)	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcEndpointServicePermissions	Grants permission to describe the principals (service consumers) that are permitted to discover your VPC endpoint service	List	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	
DescribeVpcEndpointServices	Grants permission to describe all supported AWS services that can be specified when creating a VPC endpoint	List		ec2:Region	
DescribeVpcEndpoints	Grants permission to describe one or more VPC endpoints	List		ec2:Region	
DescribeVpcPeeringConnections	Grants permission to describe one or more VPC peering connections	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcs	Grants permission to describe one or more VPCs	List		ec2:Region	
DescribeVpnConcentrators	Grants permission to describe one or more VPN concentrators	List		ec2:Region	
DescribeVpnConnections	Grants permission to describe one or more VPN connections	List		ec2:Region	
DescribeVpnGateways	Grants permission to describe one or more virtual private gateways	List		ec2:Region	
DetachApplianceFromNatGateway [permission only]	Grants permission to detach an appliance from a public/private Natgateway	Permissions management	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachClassicLinkVpc	Grants permission to unlink (detach) a linked EC2-Classic instance from a VPC	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DetachInternetGateway	Grants permission to detach an internet gateway from a VPC	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachNetworkInterface	Grants permission to detach a network interface from an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachResourcesFromPlacementGroup [permission only]	Grants permission to detach resources from a placement group	Permissions management	placement-group*	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	
DetachVerifiedAccessTrustProvider	Grants permission to detach a trust provider 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
			verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachVolume	Grants permission to detach an EBS volume from an instance	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
DetachVpnGateway	Grants permission to detach a virtual private gateway from a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableAddressTransfer	Grants permission to disable Elastic IP address transfer	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisableAllowedImagesSettings	Grants permission to disable allowed images settings	Write		ec2:Region	
DisableAwsNetworkPerformanceMetricSubscription	Grants permission to disable infrastructure performance metric subscriptions	Write		ec2:Region	
DisableCapacityManager	Grants permission to disable EC2 Capacity Manager for your account	Write		ec2:Region	
DisableEbsEncryptionByDefault	Grants permission to disable EBS encryption by default for your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableFastLaunch	Grants permission to disable faster launching for Windows AMIs	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableFastSnapshotRestores	Grants permission to disable fast snapshot restores for one or more snapshots in specified Availability Zones	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableImage	Grants permission to disable an AMI	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DisableImageBlockPublicAccess	Grants permission to disable block public access for AMIs at the account level in the specified AWS Region	Permissions management		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableImageDeprecation	Grants permission to cancel the deprecation of the specified AMI	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableImageDeregistrationProtection	Grants permission to disable deregistration protection for an AMI. When deregistration protection is disabled, the AMI can be deregistered	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableInstanceSqlHaStandbyDetections	Grants permission to disable EC2 instance SQL HA standby detections	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisableIpamOrganizationAdminAccount	Grants permission to disable an AWS Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region	organizations:DeregisterDelegatedAdministrator
DisableIpamPolicy	Grants permission to disable a policy in Amazon VPC IP Address Manager (IPAM) that controls public IPv4 address allocation	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableRouteServerPropagation	Grants permission to disable route server propagation	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DisableSerialConsoleAccess	Grants permission to disable access to the EC2 serial console of all instances for your account	Write		ec2:Region	
DisableSnapshotBlockPublicAccess	Grants permission to disable the block public access for snapshots setting for a Region	Permissions management		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableTransitGatewayRouteTablePropagation	Grants permission to disable a resource attachment from propagating routes to the specified propagation route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	
DisableVgwRoutePropagation	Grants permission to disable a virtual private gateway from propagating routes to a specified route table of a VPC	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableVpcClassicLink	Grants permission to disable ClassicLink for a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableVpcClassicLinkDnsSupport	Grants permission to disable ClassicLink DNS support for a VPC	Write	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateAddress	Grants permission to disassociate an Elastic IP address from an instance or network interface	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateCapacityReservationBillingOwner	Grants permission to cancel a pending request to assign billing of the unused capacity of a Capacity Reservation to a consumer account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateClientVpnTargetNetwork	Grants permission to disassociate a target network from a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateEnclaveCertificateIamRole	Grants permission to disassociate an ACM certificate from a IAM role	Write	certificate*		
			role*		
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIamInstanceProfile	Grants permission to disassociate an IAM instance profile from a running or stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
DisassociateInstanceEventWindow	Grants permission to disassociate one or more targets from an event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateIpamByoasn	Grants permission to disassociate an Autonomous System Number (ASN) from a BYOIP CIDR	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIpamResourceDiscovery	Grants permission to disassociate a resource discovery from an Amazon VPC IPAM	Write	ipam-resource-discovery-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateNatGatewayAddress	Grants permission to disassociate a secondary Elastic IP address from a public NAT gateway	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateRouteServer	Grants permission to disassociate a route server from a VPC	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateRouteTable	Grants permission to disassociate a subnet from a route table	Write	internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateSecurityGroupVpc	Grants permission to disassociate a security group from a VPC	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateSubnetCidrBlock	Grants permission to disassociate a CIDR block from a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayMulticastDomain	Grants permission to disassociate one or more subnets from a transit gateway multicast domain	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayPolicyTable	Grants permission to disassociate a policy table from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayRouteTable	Grants permission to disassociate a resource attachment from a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTrunkInterface	Grants permission to disassociate a branch network interface to a trunk network interface	Write		ec2:Region	
DisassociateVerifiedAccessInstanceWebAcl [permission only]	Grants permission to disassociate an AWS Web Application Firewall (WAF) web access control list (ACL) from a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateVpcCidrBlock	Grants permission to disassociate a CIDR block from a VPC	Write	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
EnableAddressTransfer	Grants permission to enable Elastic IP address transfer	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
EnableAllowedImagesSettings	Grants permission to enable allowed images settings	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableAwsNetworkPerformanceMetricSubscription	Grants permission to enable infrastructure performance subscriptions	Write		ec2:Region	
EnableCapacityManager	Grants permission to enable EC2 Capacity Manager for your account	Write		ec2:Region	
EnableEbsEncryptionByDefault	Grants permission to enable EBS encryption by default for your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFastLaunch	Grants permission to enable faster launching for Windows AMIs	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateLaunchTemplate ec2:CreateSnapshot ec2:CreateTags ec2:DeleteSnapshot ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypeOfferings ec2:DescribeInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSnapshots ec2:DescribeSubnets ec2:RunInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFastSnapshotRestores	Grants permission to enable fast snapshot restores for one or more snapshots in specified Availability Zones	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImage	Grants permission to re-enable a disabled AMI	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
EnableImageBlockPublicAccess	Grants permission to enable block public access for AMIs at the account level in the specified AWS Region	Permissions management		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImageDeprecation	Grants permission to enable deprecation of the specified AMI at the specified date and time	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImageDeregistrationProtection	Grants permission to enable deregistration protection for an AMI. When deregistration protection is enabled, the AMI can't be deregistered	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableInstanceSqlHaStandbyDetections	Grants permission to enable EC2 instance SQL HA standby detections	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
EnableIpamOrganizationAdminAccount	Grants permission to enable an AWS Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
EnableIpamPolicy	Grants permission to enable an Amazon VPC IP Address Manager (IPAM) policy	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableReachabilityAnalyzerOrganizationSharing	Grants permission to enable organization sharing of reachability analyzer	Write		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
EnableRouteServerPropagation	Grants permission to enable route server propagation	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
EnableSerialConsoleAccess	Grants permission to enable access to the EC2 serial console of all instances for your account	Write		ec2:Region	
EnableSnapshotBlockPublicAccess	Grants permission to enable or modify the block public access for snapshots setting for a Region	Permissions management		ec2:Region	
EnableTransitGatewayRouteTablePropagation	Grants permission to enable an attachment to propagate routes to a propagation route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableVgwRoutePropagation	Grants permission to enable a virtual private gateway to propagate routes to a VPC route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableVolumeIO	Grants permission to enable I/O operations for a volume that had I/O operations disabled	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
EnableVpcClassicLink	Grants permission to enable a VPC for ClassicLink	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableVpcClassicLinkDnsSupport	Grants permission to enable a VPC to support DNS hostname resolution for ClassicLink	Write	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportClientVpnClientCertificateRevocationList	Grants permission to download the client certificate revocation list for a Client VPN endpoint	Read	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportClientVpnClientConfiguration	Grants permission to download the contents of the Client VPN endpoint configuration file for a Client VPN endpoint	Read	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ExportImage	Grants permission to export an Amazon Machine Image (AMI) to a VM file	Write	export-image-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ExportTransitGatewayRoutes	Grants permission to export routes from a transit gateway route table to an Amazon S3 bucket	Write		ec2:Region	
ExportVerifiedAccessInstanceClientConfiguration	Grants permission to export a verified access instance client configuration	Read	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetActiveVpnTunnelStatus	Grants permission to retrieve the current security parameters for an active VPN tunnel	Read	vpn-connection*	ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetAllowedImagesSettings	Grants permission to get the allowed settings for images	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssociatedEnclaveCertificateIamRoles	Grants permission to get the list of roles associated with an ACM certificate	Read	certificate*		
				ec2:Region	
GetAssociatedIpv6PoolCidrs	Grants permission to get information about the IPv6 CIDR block associations for a specified IPv6 address pool	Read	ipv6pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetAwsNetworkPerformanceData	Grants permission to get network performance data	Read		ec2:Region	
GetCapacityManagerAttributes	Grants permission to retrieve the current configuration and status of EC2 Capacity Manager	Read		ec2:Region	
GetCapacityManagerMetricData	Grants permission to retrieve capacity usage metrics for your EC2 resources	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCapacityManagerMetricDimensions	Grants permission to retrieve the available dimension values for capacity metrics within a specified time range	Read		ec2:Region	
GetCapacityReservationUsage	Grants permission to get usage information about a Capacity Reservation	Read	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
GetCoipPoolUsage	Grants permission to describe the allocations from the specified customer-owned address pool	Read	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConsoleOutput	Grants permission to get the console output for an instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConsoleScreenshot	Grants permission to retrieve a JPG-format screenshot of a running instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetDeclarativePoliciesReportSummary	Grants permission to get the report summary of declarative policies	Read	declarative-policies-report*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetDefaultCreditSpecification	Grants permission to get the default credit option for CPU usage of a burstable performance instance family	Read		ec2:Region	
GetEbsDefaultKmsKeyId	Grants permission to get the ID of the default customer master key (CMK) for EBS encryption by default	Read		ec2:Region	
GetEbsEncryptionByDefault	Grants permission to describe whether EBS encryption by default is enabled for your account	Read		ec2:Region	
GetEnabledIpamPolicy	Grants permission to describe the currently enabled policy in Amazon VPC IP Address Manager (IPAM)	Read		ec2:Region	
GetFlowLogsIntegrationTemplate	Grants permission to generate a CloudFormation template to streamline the integration of VPC flow logs with Amazon Athena	Read	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetGroupsForCapacityReservation	Grants permission to list the resource groups to which a Capacity Reservation has been added	List	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
GetHostReservationPurchasePreview	Grants permission to preview a reservation purchase with configurations that match those of a Dedicated Host	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetImageAncestry	Grants permission to retrieve the ancestry chain of an AMI back to its root AMI	Read	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
GetImageBlockPublicAccessState	Grants permission to get the current state of block public access for AMIs at the account level in the specified AWS Region	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceMetadataDefaults	Grants permission to view the default instance metadata service (IMDS) settings set for your account in the specified Region	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceTpmEkPub	Grants permission to get the public endorsement key associated with the Nitro Trusted Platform Module (NitroTPM) for the specified instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetInstanceTypesFromInstanceRequirements	Grants permission to view a list of instance types with specified instance attributes	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceUefiData	Grants permission to retrieve the binary representation of the UEFI variable store	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetIpamAddressHistory	Grants permission to retrieve historical information about a CIDR within an Amazon VPC IP Address Manager (IPAM) scope	Read	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetIpamDiscoveredAccounts	Grants permission to retrieve IPAM discovered accounts	Read	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamDiscoveredPublicAddresses	Grants permission to retrieve the public IP addresses that have been discovered by IPAM	Read	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamDiscoveredResourceCidrs	Grants permission to retrieve the resource CIDRs that are monitored as part of a resource discovery	Read	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPolicyAllocationRules	Grants permission to describe the rules that define how Amazon VPC IP Address Manager (IPAM) pools allocate IP addresses to AWS resource types within an IPAM policy	List	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamPolicyOrganizationTargets	Grants permission to retrieve the AWS Organizations targets associated with an Amazon VPC IP Address Manager (IPAM) policy	List	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPoolAllocations	Grants permission to get a list of all the CIDR allocations in an Amazon VPC IP Address Manager (IPAM) pool	List	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamPoolCidrs	Grants permission to get the CIDRs provisioned to an Amazon VPC IP Address Manager (IPAM) pool	Read	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPrefixListResolverRules	Grants permission to get rules for an IPAM prefix list resolver	Read	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamPrefixListResolverVersionEntries	Grants permission to get CIDR entries for a specific version of an IPAM prefix list resolver	Read	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPrefixListResolverVersions	Grants permission to get versions of an IPAM prefix list resolver	Read	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamResourceCidrs	Grants permission to get information about the resources in an Amazon VPC IP Address Manager (IPAM) scope	Read	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLaunchTemplateData	Grants permission to get the configuration data of the specified instance for use with a new launch template or launch template version	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetManagedPrefixListAssociations	Grants permission to get information about the resources that are associated with the specified managed prefix list	Read	prefix-list*	aws:ResourceTag/${TagKey} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetManagedPrefixListEntries	Grants permission to get information about the entries for a specified managed prefix list	Read	prefix-list*	aws:ResourceTag/${TagKey} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetNetworkInsightsAccessScopeAnalysisFindings	Grants permission to get the findings for one or more Network Access Scope analyses	Read	network-insights-access-scope-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetworkInsightsAccessScopeContent	Grants permission to get the content for a specified Network Access Scope	Read	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPasswordData	Grants permission to retrieve the encrypted administrator password for a running Windows instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReservedInstancesExchangeQuote	Grants permission to return a quote and exchange information for exchanging one or more Convertible Reserved Instances for a new Convertible Reserved Instance	Read	reserved-instances*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy [permission only]	Grants permission to describe an IAM policy that enables cross-account sharing	Read	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetRouteServerAssociations	Grants permission to get associations for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRouteServerPropagations	Grants permission to get propagations for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRouteServerRoutingDatabase	Grants permission to get the routing database for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetSecurityGroupsForVpc	Grants permission to retrieve a list of security groups for a specified VPC	Read	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSerialConsoleAccessStatus	Grants permission to retrieve the access status of your account to the EC2 serial console of all instances	Read		ec2:Region	
GetSnapshotBlockPublicAccessState	Grants permission to retrieve the current state of the block public access for snapshots setting for a Region	Read		ec2:Region	
GetSpotPlacementScores	Grants permission to calculate the Spot placement score for a Region or Availability Zone based on the specified target capacity and compute requirements	Read		ec2:Region	
GetSubnetCidrReservations	Grants permission to retrieve information about the subnet CIDR reservations	Read		ec2:Region	
GetTransitGatewayAttachmentPropagations	Grants permission to list the route tables to which a resource attachment propagates routes	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransitGatewayMeteringPolicyEntries	Grants permission to list the entries for a transit gateway metering policy	List	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	
				ec2:Region	
GetTransitGatewayMulticastDomainAssociations	Grants permission to get information about the associations for a transit gateway multicast domain	List	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetTransitGatewayPolicyTableAssociations	Grants permission to get information about associations for a transit gateway policy table	List	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransitGatewayPolicyTableEntries	Grants permission to get information about associations for a transit gateway policy table entry	List	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	
GetTransitGatewayPrefixListReferences	Grants permission to get information about prefix list references for a transit gateway route table	List		ec2:Region	
GetTransitGatewayRouteTableAssociations	Grants permission to get information about associations for a transit gateway route table	List		ec2:Region	
GetTransitGatewayRouteTablePropagations	Grants permission to get information about the route table propagations for a transit gateway route table	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerifiedAccessEndpointPolicy	Grants permission to show the Verified Access policy associated with the endpoint	List	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetVerifiedAccessEndpointTargets	Grants permission to get verified access endpoint targets	List	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerifiedAccessGroupPolicy	Grants permission to show the contents of the Verified Access policy associated with the group	List	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetVerifiedAccessInstanceWebAcl [permission only]	Grants permission to show the AWS Web Application Firewall (WAF) web access control list (ACL) for a Verified Access instance	List	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVpcResourcesBlockingEncryptionEnforcement	Grants permission to describe resources that would block VPC Encryption Control enforcement	List	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
GetVpnConnectionDeviceSampleConfiguration	Grants permission to download an AWS-provided sample configuration file to be used with the customer gateway device	List	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpn-connection-device-type*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetVpnConnectionDeviceTypes	Grants permission to obtain a list of customer gateway devices for which sample configuration files can be provided	List		ec2:Region	
GetVpnTunnelReplacementStatus	Grants permission to view available tunnel endpoint maintenance events	List	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ImportByoipCidrToIpam [permission only]	Grants permission to transfer existing BYOIP IPv4 CIDRs to IPAM	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportClientVpnClientCertificateRevocationList	Grants permission to upload a client certificate revocation list to a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ImportImage	Grants permission to import single or multi-volume disk images or EBS snapshots into an Amazon Machine Image (AMI)	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:RootDeviceType	ec2:CreateTags
			import-image-task*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportInstance	Grants permission to create an import instance task using metadata from a disk image	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
ImportKeyPair	Grants permission to import a public key from an RSA key pair that was created with a third-party tool	Write	key-pair*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportSnapshot	Grants permission to import a disk into an EBS snapshot	Write	import-snapshot-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Owner ec2:ParentVolume ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportVolume	Grants permission to create an import volume task using metadata from a disk image	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
InjectApiError [permission only]	Grants permission to temporarily inject errors for target API requests	Write		ec2:FisActionId ec2:FisTargetArns ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InjectVolumeIOLatency [permission only]	Grants permission to temporarily inject latency to I/O operations for a target Amazon EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
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	
ListVolumesInRecycleBin	Grants permission to list EBS volumes in Recycle Bin	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LockSnapshot	Grants permission to lock an Amazon EBS snapshot in either governance or compliance mode to protect it against accidental or malicious deletions	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyAddressAttribute	Grants permission to modify an attribute of the specified Elastic IP address	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyAvailabilityZoneGroup	Grants permission to modify the opt-in status of the Local Zone and Wavelength Zone group for your account	Write		ec2:Region	
ModifyCapacityReservation	Grants permission to modify a Capacity Reservation's capacity and the conditions under which it is to be released	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:CapacityReservationFleet	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyCapacityReservationFleet	Grants permission to modify a Capacity Reservation Fleet	Write	capacity-reservation-fleet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	ec2:ModifyCapacityReservation
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyClientVpnEndpoint	Grants permission to modify a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:SamlProviderArn ec2:ServerCertificateArn	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
ModifyDefaultCreditSpecification	Grants permission to change the account level default credit option for CPU usage of burstable performance instances	Write		ec2:Region	
ModifyEbsDefaultKmsKeyId	Grants permission to change the default customer master key (CMK) for EBS encryption by default for your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyFleet	Grants permission to modify an EC2 Fleet	Write	fleet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyFpgaImageAttribute	Grants permission to modify an attribute of an Amazon FPGA Image (AFI)	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyHosts	Grants permission to modify a Dedicated Host	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIdFormat	Grants permission to modify the ID format for a resource	Write		ec2:Region	
ModifyIdentityIdFormat	Grants permission to modify the ID format of a resource for a specific principal in your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyImageAttribute	Grants permission to modify an attribute of an Amazon Machine Image (AMI)	Write	image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceAttribute	Grants permission to modify an attribute of an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitiali	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				zationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCapacityReservationAttributes	Grants permission to modify the Capacity Reservation settings for a stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			capacity-reservation	aws:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceConnectEndpoint	Grants permission to modify an existing EC2 Instance Connect Endpoint	Write	instance-connect-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCpuOptions	Grants permission to modify the CPU options on an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCreditSpecification	Grants permission to modify the credit option for CPU usage on an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceEventStartTime	Grants permission to modify the start time for a scheduled EC2 instance event	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceEventWindow	Grants permission to modify the specified event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMaintenanceOptions	Grants permission to modify the recovery behaviour for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMetadataDefaults	Grants permission to modify the default instance metadata service (IMDS) settings for your account in the specified Region	Write		ec2:Attribute/${AttributeName} ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMetadataOptions	Grants permission to modify the metadata options for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceNetworkPerformanceOptions	Grants permission to modify the network performance options for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstancePlacement	Grants permission to modify the placement attributes for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			dedicated-host	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpam	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM)	Write	ipam*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIpamPolicyAllocationRules	Grants permission to modify the rules that define how Amazon VPC IP Address Manager (IPAM) pools allocate IP addresses to AWS resource types within an IPAM policy	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIpamPool	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyIpamPrefixListResolver	Grants permission to modify an IPAM prefix list resolver	Write	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			ipam-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyIpamPrefixListResolverTarget	Grants permission to modify an IPAM prefix list resolver target	Write	ipam-prefix-list-resolver-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpamResourceCidr	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) resource CIDR	Write	ipam-scope*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpamResourceDiscovery	Grants permission to modify a resource discovery	Write	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpamScope	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) scope	Write	ipam-scope*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyLaunchTemplate	Grants permission to modify a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyLocalGatewayRoute	Grants permission to modify a local gateway route	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyManagedPrefixList	Grants permission to modify a managed prefix list	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyNetworkInterfaceAttribute	Grants permission to modify an attribute of a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyOdbNetworkPeering [permission only]	Grants permission to allow Oracle Database@AWS to modify the settings of a peering connection between an ODB network and a VPC	Permissions management	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyPrivateDnsNameOptions	Grants permission to modify the options for instance hostnames for the specified instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyPublicIpDnsNameOptions	Grants permission to modify public hostname options for a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyReservedInstances	Grants permission to modify attributes of one or more Reserved Instances	Write	reserved-instances*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyRouteServer	Grants permission to modify a route server	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifySecurityGroupRules	Grants permission to modify the rules of a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group-rule*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySnapshotAttribute	Grants permission to add or remove permission settings for a snapshot	Permissions management	snapshot*	aws:ResourceTag/${TagKey} ec2:Add/group ec2:Add/userId ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Owner ec2:ParentVolume ec2:Remove/group ec2:Remove/userId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySnapshotTier	Grants permission to archive Amazon EBS snapshots	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize	
				ec2:Region	
ModifySpotFleetRequest	Grants permission to modify a Spot Fleet request	Write	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySubnetAttribute	Grants permission to modify an attribute of a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorFilterNetworkServices	Grants permission to allow or restrict mirroring network services	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorFilterRule	Grants permission to modify a traffic mirror rule	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter-rule*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorSession	Grants permission to modify a traffic mirror session	Write	traffic-mirror-session*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			traffic-mirror-filter	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-target	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGateway	Grants permission to modify a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGatewayMeteringPolicy	Grants permission to modify a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGatewayPrefixListReference	Grants permission to modify a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGatewayVpcAttachment	Grants permission to modify a VPC attachment on a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessEndpoint	Grants permission to modify the configuration of a Verified Access endpoint	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyVerifiedAccessEndpointPolicy	Grants permission to modify the specified Verified Access endpoint policy	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessGroup	Grants permission to modify the specified Verified Access Group configuration	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			verified-access-instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessGroupPolicy	Grants permission to modify the specified Verified Access group policy	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessInstance	Grants permission to modify the configuration of the specified Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessInstanceLoggingConfiguration	Grants permission to modify the logging configuration for the specified Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessTrustProvider	Grants permission to modify the configuration of the specified Verified Access trust provider	Write	verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVolume	Grants permission to modify the parameters of an EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVolumeAttribute	Grants permission to modify an attribute of a volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcAttribute	Grants permission to modify an attribute of a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcBlockPublicAccessExclusion	Grants permission to modify an exclusion list for blocked public access on a VPC	Write	vpc-block-public-access-exclusion*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVpcBlockPublicAccessOptions	Grants permission to modify options for blocked public access on a VPC	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEncryptionControl	Grants permission to modify an existing VPC Encryption Control	Write	vpc-encryption-control*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpoint	Grants permission to modify an attribute of a VPC endpoint	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointConnectionNotification	Grants permission to modify a connection notification for a VPC endpoint or VPC endpoint service	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointServiceConfiguration	Grants permission to modify the attributes of a VPC endpoint service configuration	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServicePrivateDnsName ec2:VpceSupportedRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyVpcEndpointServicePayerResponsibility	Grants permission to modify the payer responsibility for a VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointServicePermissions	Grants permission to modify the permissions for a VPC endpoint service	Permissions management	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcPeeringConnectionOptions	Grants permission to modify the VPC peering connection options on one side of a VPC peering connection	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:Attribute ec2:Attribute/${AttributeName} ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcTenancy	Grants permission to modify the instance tenancy attribute of a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnConnection	Grants permission to modify the target gateway of a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnConnectionOptions	Grants permission to modify the connection options for your Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnTunnelCertificate	Grants permission to modify the certificate for a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnTunnelOptions	Grants permission to modify the options for a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MonitorInstances	Grants permission to enable detailed monitoring for a running instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
MoveAddressToVpc	Grants permission to move an Elastic IP address from the EC2-Classic platform to the EC2-VPC platform	Write		ec2:Region	
MoveByoipCidrToIpam	Grants permission to move a BYOIP IPv4 CIDR to Amazon VPC IP Address Manager (IPAM) from a public IPv4 pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MoveCapacityReservationInstances	Grants permission to move available capacity from a source Capacity Reservation to a destination Capacity Reservation	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PauseVolumeIO [permission only]	Grants permission to temporarily pause I/O operations for a target Amazon EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ProvisionByoipCidr	Grants permission to provision an address range for use in AWS through bring your own IP addresses (BYOIP), and to create a corresponding address pool	Write		ec2:Region	
ProvisionIpamByoasn	Grants permission to provision an Autonomous System Number (ASN) for use in an Amazon Web Services account	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ProvisionIpamPoolCidr	Grants permission to provision a CIDR to an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-external-resource-verification-token	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ProvisionPublicIpv4PoolCidr	Grants permission to provision a CIDR to a public IPv4 pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
PurchaseCapacityBlock	Grants permission to purchase a Capacity Block offering	Write	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:CapacityReservationFleet	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseCapacityBlockExtension	Grants permission to purchase a Capacity Block extension	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
PurchaseHostReservation	Grants permission to purchase a reservation with configurations that match those of a Dedicated Host	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
				ec2:Region	
PurchaseReservedInstancesOffering	Grants permission to purchase a Reserved Instance offering	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseScheduledInstances	Grants permission to purchase one or more Scheduled Instances with a specified schedule	Write		ec2:Region	
PutResourcePolicy [permission only]	Grants permission to attach an IAM policy that enables cross-account sharing to a resource	Permissions management	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RebootInstances	Grants permission to request a reboot of one or more instances	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
RegisterImage	Grants permission to register an Amazon Machine Image (AMI)	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterInstanceEventNotificationAttributes	Grants permission to add tags to the set of tags to include in notifications about scheduled events for your instances	Write		ec2:Region	
RegisterTransitGatewayMulticastGroupMembers	Grants permission to register one or more network interfaces as a member of a group IP address in a transit gateway multicast domain	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterTransitGatewayMulticastGroupSources	Grants permission to register one or more network interfaces as a source of a group IP address in a transit gateway multicast domain	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectCapacityReservationBillingOwnership	Grants permission to reject a request to assign billing of the available capacity of a shared Capacity Reservation to your account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectTransitGatewayMulticastDomainAssociations	Grants permission to reject requests to associate cross-account subnets with a transit gateway multicast domain	Write	transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectTransitGatewayPeeringAttachment	Grants permission to reject a transit gateway peering attachment request	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
RejectTransitGatewayVpcAttachment	Grants permission to reject a request to attach a VPC to a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RejectVpcEndpointConnections	Grants permission to reject one or more VPC endpoint connection requests to a VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectVpcPeeringConnection	Grants permission to reject a VPC peering connection request	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReleaseAddress	Grants permission to release an Elastic IP address	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
ReleaseHosts	Grants permission to release one or more On-Demand Dedicated Hosts	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReleaseIpamPoolAllocation	Grants permission to release an allocation within an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceIamInstanceProfileAssociation	Grants permission to replace an IAM instance profile for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ReplaceImageCriteriaInAllowedImagesSettings	Grants permission to replace image criteria in allowed images settings	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceNetworkAclAssociation	Grants permission to change which network ACL a subnet is associated with	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceNetworkAclEntry	Grants permission to replace an entry (rule) in a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	
ReplaceRoute	Grants permission to replace a route within a route table in a VPC	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReplaceRouteTableAssociation	Grants permission to change the route table that is associated with a subnet	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReplaceTransitGatewayRoute	Grants permission to replace a route in a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReplaceVpnTunnel	Grants permission to replace a VPN tunnel	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ReportInstanceStatus	Grants permission to submit feedback about the status of an instance	Write	instance*	ec2:AvailabilityZoneId ec2:InstanceBandwidthWeighting ec2:InstanceID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RequestSpotFleet	Grants permission to create a Spot Fleet request	Write	spot-fleet-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
RequestSpotInstances	Grants permission to create a Spot Instance request	Write	spot-instances-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetAddressAttribute	Grants permission to reset the attribute of the specified IP address	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetEbsDefaultKmsKeyId	Grants permission to reset the default customer master key (CMK) for EBS encryption for your account to use the AWS-managed CMK for EBS	Write		ec2:Region	
ResetFpgaImageAttribute	Grants permission to reset an attribute of an Amazon FPGA Image (AFI) to its default value	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetImageAttribute	Grants permission to reset an attribute of an Amazon Machine Image (AMI) to its default value	Write	image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetInstanceAttribute	Grants permission to reset an attribute of an instance to its default value	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetNetworkInterfaceAttribute	Grants permission to reset an attribute of a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetSnapshotAttribute	Grants permission to reset permission settings for a snapshot	Permissions management	snapshot*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RestoreAddressToClassic	Grants permission to restore an Elastic IP address that was previously moved to the EC2-VPC platform back to the EC2-Classic platform	Write		ec2:Region	
RestoreImageFromRecycleBin	Grants permission to restore an Amazon Machine Image (AMI) from the Recycle Bin	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RestoreManagedPrefixListVersion	Grants permission to restore the entries from a previous version of a managed prefix list to a new version of the prefix list	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreSnapshotFromRecycleBin	Grants permission to restore an Amazon EBS snapshot from the Recycle Bin	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreSnapshotTier	Grants permission to restore an archived Amazon EBS snapshot for use temporarily or permanently, or modify the restore period or restore type for a snapshot that was previously temporarily restored	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreVolumeFromRecycleBin	Grants permission to restore an EBS volume from Recycle Bin	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeClientVpnIngress	Grants permission to remove an inbound authorization rule from a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RevokeSecurityGroupEgress	Grants permission to remove one or more outbound rules from a VPC security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeSecurityGroupIngress	Grants permission to remove one or more inbound rules from a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RunInstances	Grants permission to launch one or more instances	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateTags iam:PassRole ssm:GetParameters

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AssociatePublicIpAddress ec2:AuthorizedService ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NetworkInterfaceID ec2:Subnet ec2:Vpc	
			security-group*	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate	
			elastic-gpu	aws:ResourceTag/${TagKey} ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-inference		
			group		
			key-pair	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:KeyPairName ec2:KeyPairType ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
			license-configuration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			secondary-subnet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ParentSnapshot	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-Classic-EBS		image* instance* security-group* volume* key-pair placement-group snapshot		
	SCENARIO: EC2-Classic-InstanceStore		image* instance* security-group* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-EBS		image* instance* network-interface* security-group* volume* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-EBS-Subnet		image* instance* network-interface* security-group* subnet* volume* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-InstanceStore		image* instance* network-interface* security-group* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-InstanceStore-Subnet		image* instance* network-interface* security-group* subnet* key-pair placement-group snapshot		
RunScheduledInstances	Grants permission to launch one or more Scheduled Instances	Write		ec2:Region	
SearchLocalGatewayRoutes	Grants permission to search for routes in a local gateway route table	List	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
SearchTransitGatewayMulticastGroups	Grants permission to search for groups, sources, and members in a transit gateway multicast domain	List	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchTransitGatewayRoutes	Grants permission to search for routes in a transit gateway route table	List	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendDiagnosticInterrupt	Grants permission to send a diagnostic interrupt to an Amazon EC2 instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendSpotInstanceInterruptions [permission only]	Grants permission to interrupt a Spot Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
StartDeclarativePoliciesReport	Grants permission to start a declarative policies report	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInstances	Grants permission to start a stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Tenancy	
			license-configuration		
				ec2:Region	
StartNetworkInsightsAccessScopeAnalysis	Grants permission to start a Network Access Scope analysis	Write	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			network-insights-access-scope-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkInsightsAnalysis	Grants permission to start analyzing a specified path	Write	network-insights-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			network-insights-path*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartVpcEndpointServicePrivateDnsVerification	Grants permission to start the private DNS verification process for a VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopInstances	Grants permission to stop an Amazon EBS-backed instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Terminate ClientVpn Connections	Grants permission to terminate active Client VPN endpoint connections	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Terminate Instances	Grants permission to shut down one or more instances	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnassignIpv6Addresses	Grants permission to unassign one or more IPv6 addresses from a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnassignPrivateIpAddresses	Grants permission to unassign one or more secondary private IP addresses from a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnassignPrivateNatGatewayAddress	Grants permission to unassign secondary private IPv4 addresses from a private NAT gateway	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnlockSnapshot	Grants permission to unlock a snapshot that is locked in governance mode or in compliance mode while still in the cooling-off period	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnmonitorInstances	Grants permission to disable detailed monitoring for a running instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
UpdateCapacityManagerOrganizationsAccess	Grants permission to update the Organizations access setting for EC2 Capacity Manager	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInterruptibleCapacityReservationAllocation	Grants permission to update the number of instances allocated to an interruptible reservation, allowing you to add more capacity or reclaim capacity to your source Capacity Reservation	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CreateDate ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount ec2:InstanceMatchCriteria	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstancePlatform ec2:InstanceType ec2:InterruptibleCapacityReservationId ec2:InterruptionType ec2:IsInterruptible ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:TargetInstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Tenancy	
				ec2:Region	
UpdateSecurityGroupRuleDescriptionsEgress	Grants permission to update descriptions for one or more outbound rules in a VPC security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecurityGroupRuleDescriptionsIngress	Grants permission to update descriptions for one or more inbound rules in a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
WithdrawByoipCidr	Grants permission to stop advertising an address range that was provisioned for use in AWS through bring your own IP addresses (BYOIP)	Write		ec2:Region	

Resource types defined by Amazon EC2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
elastic-ip	arn:${Partition}:ec2:${Region}:${Account}:elastic-ip/${AllocationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:Region ec2:ResourceTag/${TagKey}
capacity-block	arn:${Partition}:ec2:${Region}:${Account}:capacity-block/${CapacityBlockId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region

Resource types	ARN	Condition keys
		ec2:ResourceTag/${TagKey}
capacity-manager-data-export	arn:${Partition}:ec2:${Region}:${Account}:capacity-manager-data-export/${CapacityManagerDataExportId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
capacity-reservation-fleet	arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation-fleet/${CapacityReservationFleetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
capacity-reservation	arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation/${CapacityReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CapacityReservationFleet ec2:CommitmentDuration ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:EphemeralStorage

Resource types	ARN	Condition keys
		ec2:InstanceCount ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:InterruptibleCapacityReservationId ec2:InterruptionType ec2:IsInterruptible ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:OutpostArn ec2:PlacementGroup ec2:Region ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:TargetInstanceCount ec2:Tenancy

Resource types	ARN	Condition keys
carrier-gateway	arn:${Partition}:ec2:${Region}:${Account}:carrier-gateway/${CarrierGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:Vpc
certificate	arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}	

Resource types	ARN	Condition keys
client-vpn-endpoint	arn:${Partition}:ec2:${Region}:${Account}:client-vpn-endpoint/${ClientVpnEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:Region ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn

Resource types	ARN	Condition keys
customer-gateway	arn:${Partition}:ec2:${Region}:${Account}:customer-gateway/${CustomerGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
declarative-policies-report	arn:${Partition}:ec2:${Region}:${Account}:declarative-policies-report/${DeclarativePoliciesReportId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
dedicated-host	arn:${Partition}:ec2:${Region}:${Account}:dedicated-host/${DedicatedHostId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Quantity ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
dhcp-options	arn:${Partition}:ec2:${Region}:${Account}:dhcp-options/${DhcpOptionsId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID ec2:Region ec2:ResourceTag/${TagKey}
egress-only-internet-gateway	arn:${Partition}:ec2:${Region}:${Account}:egress-only-internet-gateway/${EgressOnlyInternetGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
elastic-gpu	arn:${Partition}:ec2:${Region}:${Account}:elastic-gpu/${ElasticGpuId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}
elastic-inference	arn:${Partition}:elastic-inference:${Region}:${Account}:elastic-inference-accelerator/${AcceleratorId}	
export-image-task	arn:${Partition}:ec2:${Region}:${Account}:export-image-task/${ExportImageTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
export-instance-task	arn:${Partition}:ec2:${Region}:${Account}:export-instance-task/${ExportTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
fleet	arn:${Partition}:ec2:${Region}:${Account}:fleet/${FleetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
fpga-image	arn:${Partition}:ec2:${Region}:${Account}:fpga-image/${FpgaImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/${TagKey}
host-reservation	arn:${Partition}:ec2:${Region}:${Account}:host-reservation/${HostReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
image	arn:${Partition}:ec2:${Region}::image/${ImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/${TagKey} ec2:RootDeviceType

Resource types	ARN	Condition keys
image-usage-report	arn:${Partition}:ec2:${Region}:${Account}:image-usage-report/${ImageUsageReportId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
import-image-task	arn:${Partition}:ec2:${Region}:${Account}:import-image-task/${ImportImageTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
import-snapshot-task	arn:${Partition}:ec2:${Region}:${Account}:import-snapshot-task/${ImportSnapshotTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
instance-connect-endpoint	arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:SubnetID
instance-event-window	arn:${Partition}:ec2:${Region}:${Account}:instance-event-window/${InstanceEventWindowId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile

Resource types	ARN	Condition keys
		ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:Region ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy

Resource types	ARN	Condition keys
internet-gateway	arn:${Partition}:ec2:${Region}:${Account}:internet-gateway/${InternetGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:InternetGatewayID ec2:Region ec2:ResourceTag/${TagKey}
ipam-external-resource-verification-token	arn:${Partition}:ec2::${Account}:ipam-external-resource-verification-token/${IpamExternalResourceVerificationTokenId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam	arn:${Partition}:ec2::${Account}:ipam/${IpamId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-policy	arn:${Partition}:ec2::${Account}:ipam-policy/${IpamPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam-pool	arn:${Partition}:ec2::${Account}:ipam-pool/${IpamPoolId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-prefix-list-resolver	arn:${Partition}:ec2::${Account}:ipam-prefix-list-resolver/${IpamPrefixListResolverId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam-prefix-list-resolver-target	arn:${Partition}:ec2::${Account}:ipam-prefix-list-resolver-target/${IpamPrefixListResolverTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-resource-discovery-association	arn:${Partition}:ec2::${Account}:ipam-resource-discovery-association/${IpamResourceDiscoveryAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam-resource-discovery	arn:${Partition}:ec2::${Account}:ipam-resource-discovery/${IpamResourceDiscoveryId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-scope	arn:${Partition}:ec2::${Account}:ipam-scope/${IpamScopeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
coip-pool	arn:${Partition}:ec2:${Region}:${Account}:coip-pool/${Ipv4PoolCoipId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipv4pool-ec2	arn:${Partition}:ec2:${Region}:${Account}:ipv4pool-ec2/${Ipv4PoolEc2Id}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipv6pool-ec2	arn:${Partition}:ec2:${Region}:${Account}:ipv6pool-ec2/${Ipv6PoolEc2Id}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
key-pair	arn:${Partition}:ec2:${Region}:${Account}:key-pair/${KeyPairName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:KeyPairName ec2:KeyPairType ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
launch-template	arn:${Partition}:ec2:${Region}:${Account}:launch-template/${LaunchTemplateId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:Region ec2:ResourceTag/${TagKey}
license-configuration	arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}	

Resource types	ARN	Condition keys
local-gateway	arn:${Partition}:ec2:${Region}:${Account}:local-gateway/${LocalGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-route-table-virtual-interface-group-association	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-virtual-interface-group-association/${LocalGatewayRouteTableVirtualInterfaceGroupAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-route-table-vpc-association	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-vpc-association/${LocalGatewayRouteTableVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
local-gateway-route-table	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table/${LocalGatewayRoutetableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-virtual-interface-group	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface-group/${LocalGatewayVirtualInterfaceGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
local-gateway-virtual-interface	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface/${LocalGatewayVirtualInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
mac-modification-task	arn:${Partition}:ec2:${Region}:${Account}:mac-modification-task/${MacModificationTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
natgateway	arn:${Partition}:ec2:${Region}:${Account}:natgateway/${NatGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:Vpc
network-acl	arn:${Partition}:ec2:${Region}:${Account}:network-acl/${NaclId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:NetworkAclID ec2:Region ec2:ResourceTag/${TagKey} ec2:Vpc

Resource types	ARN	Condition keys
network-insights-access-scope-analysis	arn:${Partition}:ec2:${Region}:${Account}:network-insights-access-scope-analysis/${NetworkInsightsAccessScopeAnalysisId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-insights-access-scope	arn:${Partition}:ec2:${Region}:${Account}:network-insights-access-scope/${NetworkInsightsAccessScopeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-insights-analysis	arn:${Partition}:ec2:${Region}:${Account}:network-insights-analysis/${NetworkInsightsAnalysisId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
network-insights-path	arn:${Partition}:ec2:${Region}:${Account}:network-insights-path/${NetworkInsightsPathId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
network-interface	arn:${Partition}:ec2:${Region}:${Account}:network-interface/${NetworkInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AssociatePublicIpAddress ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthorizedService ec2:AuthorizedUser ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:Region

Resource types	ARN	Condition keys
		ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc
outpost-lag	arn:${Partition}:ec2:${Region}:${Account}:outpost-lag/${OutpostLagId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
placement-group	arn:${Partition}:ec2:${Region}:${Account}:placement-group/${PlacementGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
prefix-list	arn:${Partition}:ec2:${Region}:${Account}:prefix-list/${PrefixListId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:IpamPrefixListResolverTargetId ec2:Region ec2:ResourceTag/${TagKey}
replace-root-volume-task	arn:${Partition}:ec2:${Region}:${Account}:replace-root-volume-task/${ReplaceRootVolumeTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
reserved-instances	arn:${Partition}:ec2:${Region}:${Account}:reserved-instances/${ReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:InstanceType ec2:Region ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy
group	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}	
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	

Resource types	ARN	Condition keys
route-server-endpoint	arn:${Partition}:ec2:${Region}:${Account}:route-server-endpoint/${RouteServerEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Region ec2:ResourceTag/${TagKey}
route-server	arn:${Partition}:ec2:${Region}:${Account}:route-server/${RouteServerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
route-server-peer	arn:${Partition}:ec2:${Region}:${Account}:route-server-peer/${RouteServerPeerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Region ec2:ResourceTag/${TagKey}
route-table	arn:${Partition}:ec2:${Region}:${Account}:route-table/${RouteTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc

Resource types	ARN	Condition keys
secondary-interface	arn:${Partition}:ec2:${Region}:${Account}:secondary-interface/${SecondaryInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}
secondary-network	arn:${Partition}:ec2:${Region}:${Account}:secondary-network/${SecondaryNetworkId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
secondary-subnet	arn:${Partition}:ec2:${Region}:${Account}:secondary-subnet/${SecondarySubnetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
security-group	arn:${Partition}:ec2:${Region}:${Account}:security-group/${SecurityGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc

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:ProductCode ec2:Region

Resource types	ARN	Condition keys
		ec2:Remove/group ec2:Remove/userId ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:SourceAvailabilityZone ec2:SourceOutpostArn ec2:VolumeSize

Resource types	ARN	Condition keys
spot-fleet-request	arn:${Partition}:ec2:${Region}:${Account}:spot-fleet-request/${SpotFleetRequestId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
spot-instances-request	arn:${Partition}:ec2:${Region}:${Account}:spot-instances-request/${SpotInstanceRequestId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
subnet-cidr-reservation	arn:${Partition}:ec2:${Region}:${Account}:subnet-cidr-reservation/${SubnetCidrReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
subnet	arn:${Partition}:ec2:${Region}:${Account}:subnet/${SubnetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc

Resource types	ARN	Condition keys
traffic-mirror-filter	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter/${TrafficMirrorFilterId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
traffic-mirror-filter-rule	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter-rule/${TrafficMirrorFilterRuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
traffic-mirror-session	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-session/${TrafficMirrorSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
traffic-mirror-target	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-target/${TrafficMirrorTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
transit-gateway-attachment	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-attachment/${TransitGatewayAttachmentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId
transit-gateway-connect-peer	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-connect-peer/${TransitGatewayConnectPeerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId

Resource types	ARN	Condition keys
transit-gateway	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway/${TransitGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayId
transit-gateway-metering-policy	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-metering-policy/${TransitGatewayMeteringPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId

Resource types	ARN	Condition keys
transit-gateway-multicast-domain	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-multicast-domain/${TransitGatewayMulticastDomainId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId
transit-gateway-policy-table	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-policy-table/${TransitGatewayPolicyTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId

Resource types	ARN	Condition keys
transit-gateway-route-table-announcement	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table-announcement/${TransitGatewayRouteTableAnnouncementId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId
transit-gateway-route-table	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table/${TransitGatewayRouteTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId

Resource types	ARN	Condition keys
verified-access-endpoint	arn:${Partition}:ec2:${Region}:${Account}:verified-access-endpoint/${VerifiedAccessEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
verified-access-endpoint-target	arn:${Partition}:ec2:${Region}:${Account}:verified-access-endpoint-target/${VerifiedAccessEndpointTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
verified-access-group	arn:${Partition}:ec2:${Region}:${Account}:verified-access-group/${VerifiedAccessGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
verified-access-policy	arn:${Partition}:ec2:${Region}:${Account}:verified-access-policy/${VerifiedAccessPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
verified-access-trust-provider	arn:${Partition}:ec2:${Region}:${Account}:verified-access-trust-provider/${VerifiedAccessTrustProviderId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
volume	arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:IsLaunchTemplateResource ec2:KmsKeyId ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType
vpc-block-public-access-exclusion	arn:${Partition}:ec2:${Region}:${Account}:vpc-block-public-access-exclusion/${VpcBlockPublicAccessExclusionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpc-encryption-control	arn:${Partition}:ec2:${Region}:${Account}:vpc-encryption-control/${VpcEncryptionControlId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
vpc-endpoint-connection	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-connection/${VpcEndpointConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpc-endpoint	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint/${VpcEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpcePrivateDnsPreference ec2:VpcePrivateDnsSpecifiedDomains ec2:VpceServiceName ec2:VpceServiceOwner ec2:VpceServiceRegion

Resource types	ARN	Condition keys
vpc-endpoint-service	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service/${VpcEndpointServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServicePrivateDnsName ec2:VpceServiceRegion ec2:VpceSupportedRegion

Resource types	ARN	Condition keys
vpc-endpoint-service-permission	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service-permission/${VpcEndpointServicePermissionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
vpc-flow-log	arn:${Partition}:ec2:${Region}:${Account}:vpc-flow-log/${VpcFlowLogId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:Region ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID

Resource types	ARN	Condition keys
vpc-peering-connection	arn:${Partition}:ec2:${Region}:${Account}:vpc-peering-connection/${VpcPeeringConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID
vpn-concentrator	arn:${Partition}:ec2:${Region}:${Account}:vpn-concentrator/${VpnConcentratorId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpn-connection-device-type	arn:${Partition}:ec2:${Region}:${Account}:vpn-connection-device-type/${VpnConnectionDeviceTypeId}	ec2:Region

Resource types	ARN	Condition keys
vpn-connection	arn:${Partition}:ec2:${Region}:${Account}:vpn-connection/${VpnConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds

Resource types	ARN	Condition keys
		ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:Region ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType

Resource types	ARN	Condition keys
vpn-gateway	`arn:${Partition}:ec2:${Region}:${Account}:vpn-gateway/${VpnGatewayId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Condition keys for Amazon EC2

Amazon EC2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
ec2:AccepterVpc	Filters access by the ARN of an accepter VPC in a VPC peering connection	ARN

Condition keys	Description	Type
ec2:Add/group	Filters access by the group being added to a snapshot	String
ec2:Add/userId	Filters access by the account id being added to a snapshot	String
ec2:AllocationId	Filters access by the allocation ID of the Elastic IP address	String
ec2:AssociatePublicIpAddress	Filters access by whether the user wants to associate a public IP address with the instance	Bool
ec2:Attribute	Filters access by an attribute of a resource	String
ec2:Attribute/${AttributeName}	Filters access by an attribute being set on a resource	String
ec2:AuthenticationType	Filters access by the authentication type for the VPN tunnel endpoints	String
ec2:AuthorizedService	Filters access by the AWS service that has permission to use a resource	String
ec2:AuthorizedUser	Filters access by an IAM principal that has permission to use a resource	String
ec2:AutoPlacement	Filters access by the Auto Placement properties of a Dedicated Host	String
ec2:AvailabilityZone	Filters access by the name of an Availability Zone in an AWS Region	String
ec2:AvailabilityZoneId	Filters access by the ID of an Availability Zone in an AWS Region	String

Condition keys	Description	Type
ec2:CapacityReservationFleet	Filters access by the ARN of the Capacity Reservation Fleet	ARN
ec2:ClientRootCertificateChainArn	Filters access by the ARN of the client root certificate chain	ARN
ec2:CloudwatchLogGroupArn	Filters access by the ARN of the CloudWatch Logs log group	ARN
ec2:CloudwatchLogStreamArn	Filters access by the ARN of the CloudWatch Logs log stream	ARN
ec2:CommitmentDuration	Filters access by commitment duration of the Capacity Reservation	Numeric
ec2:CpuOptionsAmdSevSnp	Filters access by the state of AMD SEV-SNP CPU Options. Currently, only US East (Ohio) and Europe (Ireland) are supported	String
ec2:CreateAction	Filters access by the name of a resource-creating API action	String
ec2:CreateDate	Filters access by the date and time at which the Capacity Reservation was created	Date
ec2:DPDTimeoutSeconds	Filters access by the duration after which DPD timeout occurs on a VPN tunnel	Numeric
ec2:DestinationCapacityReservationId	Filters access by the ID of the Capacity Reservation that you want to move capacity into	ARN

Condition keys	Description	Type
ec2:DhcpOptionsID	Filters access by the ID of a dynamic host configuration protocol (DHCP) options set	String
ec2:DirectoryArn	Filters access by the ARN of the directory	ARN
ec2:Domain	Filters access by the domain of the Elastic IP address	String
ec2:EbsOptimized	Filters access by whether the instance is enabled for EBS optimization	Bool
ec2:ElasticGpuType	Filters access by the type of Elastic Graphics accelerator	String
ec2:Encrypted	Filters access by whether the EBS volume is encrypted	Bool
ec2:EndDate	Filters access by the date and time at which the Capacity Reservation ends	Date
ec2:EndDateType	Filters access by the way in which the Capacity Reservation ends	String
ec2:EphemeralStorage	Filters access by whether the instance is enabled for ephemeral storage	Bool
ec2:FisActionId	Filters access by the ID of an AWS FIS action	String
ec2:FisTargetArns	Filters access by the ARN of an AWS FIS target	ArrayOfARN
ec2:GatewayType	Filters access by the gateway type for a VPN endpoint on the AWS side of a VPN connection	String
ec2:HostRecovery	Filters access by whether host recovery is enabled for a Dedicated Host	String
ec2:IKEVersions	Filters access by the internet key exchange (IKE) versions that are permitted for a VPN tunnel	ArrayOfString

Condition keys	Description	Type
ec2:ImageID	Filters access by the ID of an image	String
ec2:ImageType	Filters access by the type of image (machine, aki, or ari)	String
ec2:InsideTunnelCidr	Filters access by the range of inside IP addresses for a VPN tunnel	String
ec2:InsideTunnelIpv6Cidr	Filters access by a range of inside IPv6 addresses for a VPN tunnel	String
ec2:InstanceAutoRecovery	Filters access by whether the instance type supports auto recovery	String
ec2:InstanceBandwidthWeighting	Filters access by the bandwidth weighting of an instance	String
ec2:InstanceCount	Filters access by the number of instances	Numeric
ec2:InstanceID	Filters access by the ID of an instance	String
ec2:InstanceMarketType	Filters access by the market or purchasing option of an instance (capacity-block, on-demand, or spot)	String
ec2:InstanceMatchCriteria	Filters access by the type of instance launches that the Capacity Reservation accepts	String
ec2:InstanceMetadataTags	Filters access by whether the instance allows access to instance tags from the instance metadata	String
ec2:InstancePlatform	Filters access by the type of operating system for which the Capacity Reservation reserves capacity	ARN
ec2:InstanceProfile	Filters access by the ARN of an instance profile	ARN

Condition keys	Description	Type
ec2:InstanceType	Filters access by the type of instance	String
ec2:InternetGatewayID	Filters access by the ID of an internet gateway	String
ec2:InterruptibleCapacityReservationId	Filters access by the ID of an interruptible Capacity Reservation	String
ec2:InterruptionType	Filters access by the type of interruption	String
ec2:IpamPrefixListResolverTargetId	Filters access by the IPAM prefix list resolver target ID that is syncing CIDRs to a managed prefix list	String
ec2:Ipv4IpamPoolId	Filters access by the ID of an IPAM pool provided for IPv4 CIDR block allocation	String
ec2:Ipv6IpamPoolId	Filters access by the ID of an IPAM pool provided for IPv6 CIDR block allocation	String
ec2:IsInterruptible	Filters access by whether Capacity Reservations are interruptible	Bool
ec2:IsLaunchTemplateResource	Filters access by whether users are able to override resources that are specified in the launch template	Bool
ec2:KeyPairName	Filters access by the name of a key pair	String
ec2:KeyPairType	Filters access by the type of a key pair	String

Condition keys	Description	Type
ec2:KmsKeyId	Filters access by the ID of an AWS KMS key provided in the request	String
ec2:LaunchTemplate	Filters access by the ARN of a launch template	ARN
ec2:Location	Filters access by the destination for the snapshot copy	String
ec2:ManagedResourceOperator	Filters access by the presence of an EC2 operator provisioning a managed resource	String
ec2:MetadataHttpEndpoint	Filters access by whether the HTTP endpoint is enabled for the instance metadata service	String
ec2:MetadataHttpPutResponseHopLimit	Filters access by the allowed number of hops when calling the instance metadata service	Numeric
ec2:MetadataHttpTokens	Filters access by whether tokens are required when calling the instance metadata service (optional or required)	String
ec2:NetworkAclID	Filters access by the ID of a network access control list (ACL)	String
ec2:NetworkInterfaceID	Filters access by the ID of an elastic network interface	String
ec2:NewInstanceProfile	Filters access by the ARN of the instance profile being attached	ARN
ec2:OutpostArn	Filters access by the ARN of the Outpost	ARN
ec2:Owner	Filters access by the owner of the resource (amazon, aws-marketplace, or an AWS account ID)	String

Condition keys	Description	Type
ec2:ParentSnapshot	Filters access by the ARN of the parent snapshot	ARN
ec2:ParentVolume	Filters access by the ARN of the parent volume from which the snapshot was created	ARN
ec2:Permission	Filters access by the type of permission for a resource (INSTANCE-ATTACH or EIP-ASSOCIATE)	String
ec2:Phase1DHGroup	Filters access by the Diffie-Hellman group numbers that are permitted for a VPN tunnel for the phase 1 IKE negotiations	ArrayOfString
ec2:Phase1EncryptionAlgorithms	Filters access by the encryption algorithms that are permitted for a VPN tunnel for the phase 1 IKE negotiations	ArrayOfString
ec2:Phase1IntegrityAlgorithms	Filters access by the integrity algorithms that are permitted for a VPN tunnel for the phase 1 IKE negotiations	ArrayOfString
ec2:Phase1LifetimeSeconds	Filters access by the lifetime in seconds for phase 1 of the IKE negotiations for a VPN tunnel	Numeric
ec2:Phase2DHGroup	Filters access by the Diffie-Hellman group numbers that are permitted for a VPN tunnel for the phase 2 IKE negotiations	ArrayOfString
ec2:Phase2EncryptionAlgorithms	Filters access by the encryption algorithms that are permitted for a VPN tunnel for the phase 2 IKE negotiations	ArrayOfString
ec2:Phase2IntegrityAlgorithms	Filters access by the integrity algorithms that are permitted for a VPN tunnel for the phase 2 IKE negotiations	ArrayOfString

Condition keys	Description	Type
ec2:Phase2LifetimeSeconds	Filters access by the lifetime in seconds for phase 2 of the IKE negotiations for a VPN tunnel	Numeric
ec2:PlacementGroup	Filters access by the ARN of the placement group	ARN
ec2:PlacementGroupName	Filters access by the name of a placement group	String
ec2:PlacementGroupStrategy	Filters access by the instance placement strategy used by the placement group (cluster, spread, or partition)	String
ec2:ProductCode	Filters access by the product code that is associated with the AMI	String
ec2:Public	Filters access by whether the image has public launch permissions	Bool
ec2:PublicIpAddress	Filters access by a public IP address	String
ec2:Quantity	Filters access by the number of Dedicated Hosts in a request	Numeric
ec2:Region	Filters access by the name of the AWS Region	String
ec2:RekeyFuzzPercentage	Filters access by the percentage of increase of the rekey window (determined by the rekey margin time) within which the rekey time is randomly selected for a VPN tunnel	Numeric
ec2:RekeyMarginTimeSeconds	Filters access by the margin time before the phase 2 lifetime expires for a VPN tunnel	Numeric

Condition keys	Description	Type
ec2:Remove/group	Filters access by the group being removed from a snapshot	String
ec2:Remove/userId	Filters access by the account id being removed from a snapshot	String
ec2:ReplayWindowSizePackets	Filters access by the number of packets in an IKE replay window	String
ec2:RequesterVpc	Filters access by the ARN of a requester VPC in a VPC peering connection	ARN
ec2:ReservedInstancesOfferingType	Filters access by the payment option of the Reserved Instance offering (No Upfront, Partial Upfront, or All Upfront)	String
ec2:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
ec2:RoleDelivery	Filters access by the version of the instance metadata service for retrieving IAM role credentials for EC2	Numeric
ec2:RootDeviceType	Filters access by the root device type of the instance (ebs or instance-store)	String
ec2:RouteTableID	Filters access by the ID of a route table	String
ec2:RoutingType	Filters access by the routing type for the VPN connection	String
ec2:SamlProviderArn	Filters access by the ARN of the IAM SAML identity provider	ARN

Condition keys	Description	Type
ec2:SecurityGroupID	Filters access by the ID of a security group	String
ec2:ServerCertificateArn	Filters access by the ARN of the server certificate	ARN
ec2:SnapshotCoolOffPeriod	Filters access by the compliance mode cooling-off period	Numeric
ec2:SnapshotID	Filters access by the ID of a snapshot	String
ec2:SnapshotLockDuration	Filters access by the snapshot lock duration	Numeric
ec2:SnapshotTime	Filters access by the initiation time of a snapshot	String
ec2:SourceAvailabilityZone	Filters access by the name of the Availability Zone from which the request originated	String
ec2:SourceCapacityReservationId	Filters access by the ID of the Capacity Reservation from which you want to move capacity	ARN
ec2:SourceInstanceARN	Filters access by the ARN of the instance from which the request originated	ARN
ec2:SourceOutpostArn	Filters access by the ARN of the Outpost from which the request originated	ARN
ec2:Subnet	Filters access by the ARN of the subnet	ARN
ec2:SubnetID	Filters access by the ID of a subnet	String
ec2:TargetInstanceCount	Filters access by the number of instances the interruptible Capacity Reservation is assigned	Numeric

Condition keys	Description	Type
ec2:Tenancy	Filters access by the tenancy of the VPC or instance (default, dedicated, or host)	String
ec2:VolumeID	Filters access by the ID of a volume	String
ec2:VolumeInitializationRate	Filters access by the initialization rate of the volume, in MiBps	Numeric
ec2:VolumeIops	Filters access by the the number of input/output operations per second (IOPS) provisioned for the volume	Numeric
ec2:VolumeSize	Filters access by the size of the volume, in GiB	Numeric
ec2:VolumeThroughput	Filters access by the throughput of the volume, in MiBps	Numeric
ec2:VolumeType	Filters access by the type of volume (gp2, gp3, io1, io2, st1, sc1, or standard)	String
ec2:Vpc	Filters access by the ARN of the VPC	ARN
ec2:VpcID	Filters access by the ID of a virtual private cloud (VPC)	String
ec2:VpcPeeringConnectionID	Filters access by the ID of a VPC peering connection	String
ec2:VpceMultiRegion	Filters access by multi region of the VPC endpoint service	String
ec2:VpcePrivateDnsPreference	Filters access by the private DNS preference	String

Condition keys	Description	Type
ec2:VpcePrivateDnsSpecifiedDomains	Filters access by the private DNS domains	ArrayOfString
ec2:VpceServiceName	Filters access by the name of the VPC endpoint service	String
ec2:VpceServiceOwner	Filters access by the service owner of the VPC endpoint service (amazon, aws-marketplace, or an AWS account ID)	String
ec2:VpceServicePrivateDnsName	Filters access by the private DNS name of the VPC endpoint service	String
ec2:VpceServiceRegion	Filters access by the region of the VPC endpoint service	String
ec2:VpceSupportedRegion	Filters access by the supported region of the VPC endpoint service	String
ec2:transitGatewayAttachmentId	Filters access by the ID of a transit gateway attachment	String
ec2:transitGatewayConnectPeerId	Filters access by the ID of a transit gateway connect peer	String
ec2:transitGatewayId	Filters access by the ID of a transit gateway	String
ec2:transitGatewayMeteringPolicyId	Filters access by the ID of a metering policy id	String

Condition keys	Description	Type
ec2:transitGatewayMulticastDomainId	Filters access by the ID of a transit gateway multicast domain	String
ec2:transitGatewayPolicyTableId	Filters access by the ID of a transit gateway policy table	String
ec2:transitGatewayRouteTableAnnouncementId	Filters access by the ID of a transit gateway route table announcement	String
ec2:transitGatewayRouteTableId	Filters access by the ID of a transit gateway route table	String

Actions, resources, and condition keys for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling (service prefix: `autoscaling`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EC2 Auto Scaling
- Resource types defined by Amazon EC2 Auto Scaling
- Condition keys for Amazon EC2 Auto Scaling

Actions defined by Amazon EC2 Auto Scaling

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachInstances	Grants permission to attach one or more EC2 instances to the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	Grants permission to attach one or more target groups to the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachLoadBalancers	Grants permission to attach one or more load balancers to the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Grants permission to attach one or more traffic sources to an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteScheduledAction	Grants permission to delete the specified scheduled actions	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
BatchPutScheduledUpdateGroupAction	Grants permission to create or update multiple scheduled scaling actions for an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CancelInstanceRefresh	Grants permission to cancel an instance refresh operation in progress	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteLifecycleAction	Grants permission to complete the lifecycle action for the specified token or instance with the specified result	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateAutoScalingGroup	Grants permission to create an Auto Scaling group with the specified name and attributes	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:ImageId autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBa	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lancerNames autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLaunchConfiguration	Grants permission to create a launch configuration	Write	launchConfiguration*		
				autoscaling:ImageId	
				autoscaling:InstanceType	
				autoscaling:SpotPrice	
				autoscaling:MetadataHttpTokens	
				autoscaling:MetadataHttpPutResponseHopLimit	
				autoscaling:MetadataHttpEndpoint	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOrUpdateTags	Grants permission to create or update tags for the specified Auto Scaling group	Tagging	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Grants permission to delete the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ForceDelete autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLaunchConfiguration	Grants permission to delete the specified launch configuration	Write	launchConfiguration*		
DeleteLifecycleHook	Grants permission to deletes the specified lifecycle hook	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	Grants permission to delete the specified notification	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicy	Grants permission to delete the specified Auto Scaling policy	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteScheduledAction	Grants permission to delete the specified scheduled action	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	Grants permission to delete the specified tags	Tagging	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWarmPool	Grants permission to delete the warm pool associated with the Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	Grants permission to describe the current Auto Scaling resource limits for your AWS account	List			
DescribeAccountSettings	Grants permission to describe the current Amazon EC2 Auto Scaling account settings for your account	List			
DescribeAdjustmentTypes	Grants permission to describe the policy adjustment types for use with PutScalingPolicy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAutoScalingGroups	Grants permission to describe one or more Auto Scaling groups. If a list of names is not provided, the call describes all Auto Scaling groups	List			
DescribeAutoScalingInstances	Grants permission to describe one or more Auto Scaling instances. If a list is not provided, the call describes all instances	List			
DescribeAutoScalingNotificationTypes	Grants permission to describe the notification types that are supported by Auto Scaling	List			
DescribeInstanceRefreshes	Grants permission to describe one or more instance refreshes for an Auto Scaling group	List			
DescribeLaunchConfigurations	Grants permission to describe one or more launch configurations. If you omit the list of names, then the call describes all launch configurations	List			
DescribeLifecycleHookTypes	Grants permission to describe the available types of lifecycle hooks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLifecycleHooks	Grants permission to describe the lifecycle hooks for the specified Auto Scaling group	List			
DescribeLoadBalancerTargetGroups	Grants permission to describe the target groups for the specified Auto Scaling group	List			
DescribeLoadBalancers	Grants permission to describe the load balancers for the specified Auto Scaling group	List			
DescribeMetricCollectionTypes	Grants permission to describe the available CloudWatch metrics for Auto Scaling	List			
DescribeNotificationConfigurations	Grants permission to describe the notification actions associated with the specified Auto Scaling group	List			
DescribePolicies	Grants permission to describe the policies for the specified Auto Scaling group	List			
DescribeScalingActivities	Grants permission to describe one or more scaling activities for the specified Auto Scaling group	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScalingProcessTypes	Grants permission to describe the scaling process types for use with ResumeProcesses and SuspendProcesses	List			
DescribeScheduledActions	Grants permission to describe the actions scheduled for your Auto Scaling group that haven't run	List			
DescribeTags	Grants permission to describe the specified tags	Read			
DescribeTerminationPolicyTypes	Grants permission to describe the termination policies supported by Auto Scaling	List			
DescribeTrafficSources	Grants permission to describe the target groups for the specified Auto Scaling group	List			
DescribeWarmPool	Grants permission to describe the warm pool associated with the Auto Scaling group	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachInstances	Grants permission to remove one or more instances from the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	Grants permission to detach one or more target groups from the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachLoadBalancers	Grants permission to remove one or more load balancers from the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Grants permission to detach one or more traffic sources from an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableMetricsCollection	Grants permission to disable monitoring of the specified metrics for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnableMetricsCollection	Grants permission to enable monitoring of the specified metrics for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	Grants permission to move the specified instances into Standby mode	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExecutePolicy	Grants permission to execute the specified policy	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExitStandby	Grants permission to move the specified instances out of Standby mode	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	Grants permission to retrieve the forecast data for a predictive scaling policy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LaunchInstances	Grants permission to launch one or more EC2 instances in the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutAccountSetting	Grants permission to modify an account setting for your account	Write			
PutLifecycleHook	Grants permission to create or update a lifecycle hook for the specified Auto Scaling Group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutNotificationConfiguration	Grants permission to configure an Auto Scaling group to send notifications when specified events take place	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Grants permission to create or update a policy for an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScheduledUpdateGroupAction	Grants permission to create or update a scheduled scaling action for an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	Grants permission to create or update the warm pool associated with the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RecordLifecycleActionHeartbeat	Grants permission to record a heartbeat for the lifecycle action associated with the specified token or instance	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResumeProcesses	Grants permission to resume the specified suspended Auto Scaling processes, or all suspended process, for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	Grants permission to rollback an instance refresh operation in progress	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetDesiredCapacity	Grants permission to set the size of the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetInstanceHealth	Grants permission to set the health status of the specified instance	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	Grants permission to update the instance protection settings of the specified instances	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartInstanceRefresh	Grants permission to start a new instance refresh operation	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:ImageId	
SuspendProcesses	Grants permission to suspend the specified Auto Scaling processes, or all processes, for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	Grants permission to terminate the specified instance and optionally adjust the desired group size	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAutoScalingGroup	Grants permission to update the configuration for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:ImageId autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:MaxSize autoscaling:MinSize autoscaling:VPCZoneIdentifiers	

Resource types defined by Amazon EC2 Auto Scaling

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
autoScalingGroup	`arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}`	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}
launchConfiguration	`arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${`	

Resource types	ARN	Condition keys
	`Id}:launchConfigurationName/${Launch ConfigurationName}`	

Condition keys for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
autoscaling:CapacityReservationIds	Filters access based on the Capacity Reservation IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	Filters access based on the ARN of a Capacity Reservation resource group	ArrayOfString
autoscaling:ForceDelete	Filters access based on whether the force delete option is specified when deleting an Auto Scaling group	Bool
autoscaling:ImageId	Filters access based on the AMI ID for the launch configuration	String
autoscaling:InstanceType	Filters access based on the instance type for the launch configuration	String

Condition keys	Description	Type
autoscaling:InstanceTypes	Filters access based on the instance types present as overrides to a launch template for a mixed instances policy. Use it to qualify which instance types can be explicitly defined in the policy	String
autoscaling:LaunchConfigurationName	Filters access based on the name of a launch configuration	String
autoscaling:LaunchTemplateVersionSpecified	Filters access based on whether users can specify any version of a launch template or only the Latest or Default version	Bool
autoscaling:LoadBalancerNames	Filters access based on the name of the load balancer	ArrayOfString
autoscaling:MaxSize	Filters access based on the maximum scaling size in the request	Numeric
autoscaling:MetadataHttpEndpoint	Filters access based on whether the HTTP endpoint is enabled for the instance metadata service	String
autoscaling:MetadataHttpPutResponseHopLimit	Filters access based on the allowed number of hops when calling the instance metadata service	Numeric
autoscaling:MetadataHttpTokens	Filters access based on whether tokens are required when calling the instance metadata service (optional or required)	String

Condition keys	Description	Type
autoscaling:MinSize	Filters access based on the minimum scaling size in the request	Numeric
autoscaling:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
autoscaling:SpotPrice	Filters access based on the price for Spot Instances for the launch configuration	Numeric
autoscaling:TargetGroupARNs	Filters access based on the ARN of a target group	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	Filters access based on the identifiers of the traffic sources	ArrayOfString
autoscaling:VPCZoneIdentifiers	Filters access based on the identifier of a VPC zone	ArrayOfString
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon EC2 Image Builder

Amazon EC2 Image Builder (service prefix: `imagebuilder`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by Amazon EC2 Image Builder

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelImageCreation	Grants permission to cancel an image creation	Write	image*		
CancelLifecycleExecution	Grants permission to cancel a lifecycle execution	Write	lifecycleExecution*		
CreateComponent	Grants permission to create a new component	Write	component*		imagebuilder:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContainerRecipe	Grants permission to create a new Container Recipe	Write	containerRecipe*		ec2:DescribeImages ecr:DescribeImages ecr:DescribeRepositories imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetObject s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDistributionConfiguration	Grants permission to create a new distribution configuration	Write	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate imagebuilder:TagResource s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImage	Grants permission to create a new image	Write	image*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					frastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImagePipeline	Grants permission to create a new image pipeline	Write	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					frastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImageRecipe	Grants permission to create a new Image Recipe	Write	imageRecipe*		ec2:DescribeImages imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInfrastructureConfiguration	Grants permission to create a new infrastructure configuration	Write	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole imagebuilder:TagResource resource-groups:GetGroup sns:Publish

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLifecyclePolicy	Grants permission to create a new lifecycle policy	Write	lifecyclePolicy*		iam:PassRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflow	Grants permission to create a new workflow	Write	workflow*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponent	Grants permission to delete a component	Write	component*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContainerRecipe	Grants permission to delete a container recipe	Write	containerRecipe*		
DeleteDistributionConfiguration	Grants permission to delete a distribution configuration	Write	distributionConfiguration*		
DeleteImage	Grants permission to delete an image	Write	image*		
DeleteImagePipeline	Grants permission to delete an image pipeline	Write	imagePipeline*		
DeleteImageRecipe	Grants permission to delete an image recipe	Write	imageRecipe*		
DeleteInfrastructureConfiguration	Grants permission to delete an infrastructure configuration	Write	infrastructureConfiguration*		
DeleteLifecyclePolicy	Grants permission to delete a lifecycle policy	Write	lifecyclePolicy*		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DistributeImage	Grants permission to distribute an image	Write	image*		ec2:DescribeImages iam:PassRole imagebuilder:GetDistributionConfiguration imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	
GetComponent	Grants permission to view details about a component	Read	component*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetComponentPolicy	Grants permission to view the resource policy associated with a component	Read	component*		
GetContainerRecipe	Grants permission to view details about a container recipe	Read	containerRecipe*		
GetContainerRecipePolicy	Grants permission to view the resource policy associated with a container recipe	Read	containerRecipe*		
GetDistributionConfiguration	Grants permission to view details about a distribution configuration	Read	distributionConfiguration*		
GetImage	Grants permission to view details about an image	Read	image*		
GetImagePipeline	Grants permission to view details about an image pipeline	Read	imagePipeline*		
GetImagePolicy	Grants permission to view the resource policy associated with an image	Read	image*		
GetImageRecipe	Grants permission to view details about an image recipe	Read	imageRecipe*		
GetImageRecipePolicy	Grants permission to view the resource policy associated with an image recipe	Read	imageRecipe*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInfrastructureConfiguration	Grants permission to view details about an infrastructure configuration	Read	infrastructureConfiguration*		
GetLifecycleExecution	Grants permission to view details about a lifecycle execution	Read	lifecycleExecution*		
GetLifecyclePolicy	Grants permission to view details about a lifecycle policy	Read	lifecyclePolicy*		
GetMarketplaceResource	Grants permission to retrieve Marketplace provided resource	Read	component*		
GetWorkflow	Grants permission to view details about a workflow	Read	workflow*		kms:Decrypt
GetWorkflowExecution	Grants permission to view details about a workflow execution	Read	workflowExecution*		
GetWorkflowStepExecution	Grants permission to view details about a workflow step execution	Read	workflowStepExecution*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportComponent	Grants permission to import a new component	Write	component *		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportDiskImage	Grants permission to import a disk image	Write	imageVersion*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportVmImage	Grants permission to import an image	Write	imageVersion*		ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
ListComponentBuildVersions	Grants permission to list the component build versions in your account	List	allComponentBuildVersions*		
ListComponents	Grants permission to list the component versions owned by or shared with your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContainerRecipes	Grants permission to list the container recipes owned by or shared with your account	List			
ListDistributionConfigurations	Grants permission to list the distribution configurations in your account	List			
ListImageBuildVersions	Grants permission to list the image build versions in your account	List	allImageBuildVersions*		
ListImagePackages	Grants permission to return a list of packages installed on the specified image	List	image*		
ListImagePipelineImages	Grants permission to return a list of images created by the specified pipeline	List	imagePipeline*		
ListImagePipelines	Grants permission to list the image pipelines in your account	List			
ListImageRecipes	Grants permission to list the image recipes owned by or shared with your account	List			
ListImageScanFindingAggregations	Grants permission to list aggregations on the image scan findings in your account	List	image imagePipeline		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImageScanFindings	Grants permission to list the image scan findings for the images in your account	List	image		inspector2:ListFindings
			imagePipeline		
ListImages	Grants permission to list the image versions owned by or shared with your account	List			
ListInfrastructureConfigurations	Grants permission to list the infrastructure configurations in your account	List			
ListLifecycleExecutionResources	Grants permission to list resources for the specified lifecycle execution	List	lifecycleExecution*		
ListLifecycleExecutions	Grants permission to list lifecycle executions for the specified resource	List	image		
			lifecyclePolicy		
ListLifecyclePolicies	Grants permission to list the lifecycle policies in your account	List			
ListTagsForResource	Grants permission to list tags for an Image Builder resource	Read	component		
			containerRecipe		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
ListWaitingWorkflowSteps	Grants permission to list waiting workflow steps for the caller account	List			
ListWorkflowBuildVersions	Grants permission to list the workflow build versions in your account	List	allWorkflowBuildVersions*		
ListWorkflowExecutions	Grants permission to list workflow executions for the specified image	List	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkflowStepExecutions	Grants permission to list workflow step executions for the specified workflow	List	workflowExecution*		kms:Decrypt
ListWorkflows	Grants permission to list the workflow versions owned by or shared with your account	List			
PutComponentPolicy	Grants permission to set the resource policy associated with a component	Permissions management	component*		
PutContainerRecipePolicy	Grants permission to set the resource policy associated with a container recipe	Permissions management	containerRecipe*		
PutImagePolicy	Grants permission to set the resource policy associated with an image	Permissions management	image*		
PutImageRecipePolicy	Grants permission to set the resource policy associated with an image recipe	Permissions management	imageRecipe*		
RetryImage	Grants permission to retry an image creation	Write	image*		
SendWorkflowStepAction	Grants permission to send an action to a workflow step	Write	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workflowStepExecution*		
StartImagePipelineExecution	Grants permission to create a new image from a pipeline	Write	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartResourceStateUpdate	Grants permission to start a state update for the specified resource	Write	image*		
TagResource	Grants permission to tag an Image Builder resource	Tagging	component		
			containerRecipe		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag an Image Builder resource	Tagging	component		
			containerRecipe		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDistributionConfiguration	Grants permission to update an existing distribution configuration	Write	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate s3:ListBucket ssm:GetParameter

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateImagePipeline	Grants permission to update an existing image pipeline	Write	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					frastructureConfiguration imagebuilder:GetWorkflow inspector2:BatchGetAccountStatus
UpdateInfrastructureConfiguration	Grants permission to update an existing infrastructure configuration	Write	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole resource-groups:GetGroup sns:Publish

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	
UpdateLifecyclePolicy	Grants permission to update an existing lifecycle policy	Write	lifecyclePolicy*		iam:PassRole
				imagebuilder:LifecyclePolicyResourceType	

Resource types defined by Amazon EC2 Image Builder

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
component	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}`	aws:ResourceTag/${TagKey}
distributionConfiguration	`arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}`	aws:ResourceTag/${TagKey}
image	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}`	aws:ResourceTag/${TagKey}
imageVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}`	aws:ResourceTag/${TagKey}
imageRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}`	aws:ResourceTag/${TagKey}
containerRecipe	`arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}	
workflowStepExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}	
allComponentBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/*	

Resource types	ARN	Condition keys
allImageBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/*	
allWorkflowBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/*	

Condition keys for Amazon EC2 Image Builder

Amazon EC2 Image Builder defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
imagebuilder:CreatedResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource created by Image Builder	String

Condition keys	Description	Type
imagebuilder:CreatedResourceTagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	Filters access by the EC2 Instance Metadata HTTP Token Requirement specified in the request	String
imagebuilder:LifecyclePolicyResourceType	Filters access by the Lifecycle Policy Resource Type specified in the request	String
imagebuilder:StatusTopicArn	Filters access by the SNS Topic Arn in the request to which terminal state notifications will be published	ARN

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				connect:privateIpAddress ec2-instance-connect: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}
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 AWS 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

Condition keys	Description	Type
ec2-instance-connect:remotePort	Filters access by port number associated with the instance	Numeric
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 ECS MCP Service

Amazon ECS MCP Service (service prefix: `ecs-mcp`) 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 ECS MCP Service
- Resource types defined by Amazon ECS MCP Service
- Condition keys for Amazon ECS MCP Service

Actions defined by Amazon ECS MCP Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvokeReadOnlyTools	Grants permission to call read-only tools in MCP service	Read			
UseMcp	Grants permission to use MCP service	Read			

Resource types defined by Amazon ECS MCP Service

Amazon ECS MCP Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon ECS MCP Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon ECS MCP Service

ECS MCP has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoleForPodIdentity	Grants permission to exchange a Kubernetes service account token for temporary AWS 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 AWS 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 EKS MCP Server

Amazon EKS MCP Server (service prefix: `eks-mcp`) 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 MCP Server

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CallPrivilegedTool	Grants permission to call privileged tools in MCP service	Write			
CallReadOnlyTool	Grants permission to call read-only tools in MCP service	Read			
InvokeMcp	Grants permission to use MCP service	Read			

Resource types defined by Amazon EKS MCP Server

Amazon EKS MCP Server does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon EKS MCP Server, specify `"Resource": "*"` in your policy.

Condition keys for Amazon EKS MCP Server

EKS MCP has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Elastic Beanstalk

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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 AWS 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 AWS 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 AWS 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 AWS Elastic Beanstalk

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteSnapshot	Grants permission to seal and complete the snapshot after all of the required blocks of data have been written to it	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Grants permission to return the data of a block in an Amazon Elastic Block Store (EBS) snapshot	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	Grants permission to list the blocks that are different between two Amazon Elastic Block Store (EBS) snapshots of the same volume/snapshot lineage	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks		Read	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to list the blocks in an Amazon Elastic Block Store (EBS) snapshot			aws:ResourceTag/${TagKey}	
PutSnapshotBlock	Grants permission to write a block of data to a snapshot created by the StartSnapshot operation	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
StartSnapshot	Grants permission to create a new EBS snapshot	Write	snapshot		ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Resource types defined by Amazon Elastic Block Store

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Condition keys for Amazon Elastic Block Store

Amazon Elastic Block Store defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Condition keys	Description	Type
ebs:Description	Filters access by the description of the snapshot being created	String
ebs:ParentSnapshot	Filters access by the ARN of the parent snapshot	ARN
ebs:VolumeSize	Filters access by the size of the volume for the snapshot being created, in GiB	Numeric

Actions, resources, and condition keys for Amazon Elastic Container Registry

Amazon Elastic Container Registry (service prefix: `ecr`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic Container Registry
- Resource types defined by Amazon Elastic Container Registry
- Condition keys for Amazon Elastic Container Registry

Actions defined by Amazon Elastic Container Registry

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCheckLayerAvailability	Grants permission to check the availability of multiple image layers in a specified registry and repository	Read	repository*		
BatchDeleteImage	Grants permission to delete a list of specified images within a specified repository	Write	repository*		
BatchGetImage	Grants permission to get detailed information for specified images within a specified repository	Read	repository*		
BatchGetRepositoryScanningConfiguration	Grants permission to retrieve repository scanning configuration for a list of repositories	Read	repository*		
BatchImportUpstreamImage [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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePullThroughCacheRule	Grants permission to create new pull-through cache rule	Write			iam:CreateServiceLinkedRole
CreateRepository	Grants permission to create an image repository	Write	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRepositoryCreationTemplate	Grants permission to create the repository creation template	Write			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLifecyclePolicy	Grants permission to delete the specified lifecycle policy	Write	repository*		
DeletePullThroughCacheRule	Grants permission to delete the pull-through cache rule	Write			
DeleteRegistryPolicy	Grants permission to delete the registry policy	Permissions management			
DeleteRepository	Grants permission to delete an existing image repository	Write	repository*		
DeleteRepositoryCreationTemplate	Grants permission to delete the repository creation template	Write			
DeleteRepositoryPolicy	Grants permission to delete the repository policy from a specified repository	Permissions management	repository*		
DeleteSigningConfiguration	Grants permission to delete the signing configuration for the registry	Write			
DeregisterPullTimeUpdateExclusion	Grants permission to deregister a pull time update exclusion	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageReplicationStatus	Grants permission to retrieve replication status about an image in a registry, including failure reason if replication fails	Read	repository*		
DescribeImageScanFindings	Grants permission to describe the image scan findings for the specified image	Read	repository*		
DescribeImageSigningStatus	Grants permission to retrieve signing status about an image in a specified registry	Read	repository*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRegistryScanningConfiguration	Grants permission to retrieve registry scanning configuration	Read			
GetRepositoryPolicy	Grants permission to retrieve the repository policy for a specified repository	Read	repository*		
GetSigningConfiguration	Grants permission to retrieve the signing configuration for the registry	Read			
InitiateLayerUpload	Grants permission to notify Amazon ECR that you intend to upload an image layer	Write	repository*		
ListImages	Grants permission to list all the image IDs for a given repository	List	repository*		
ListPullTimeUpdateExclusions	Grants permission to list pull time update exclusions for the registry	List			
ListTagsForResource	Grants permission to list the tags for an Amazon ECR resource	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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
PutSigningConfiguration	Grants permission to update the signing configuration for the registry	Write			
RegisterPullTimeUpdateExclusion	Grants permission to register a pull time update exclusion	Write			
ReplicateImage [permission only]	Grants permission to replicate images to the destination registry	Write	repository*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartLifecyclePolicyPreview	Grants permission to start a preview of the specified lifecycle policy	Write	repository*		
TagResource	Grants permission to tag an Amazon ECR resource	Tagging	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag an Amazon ECR resource	Tagging	repository*		
				aws:TagKeys	
UpdateImageStorageClass	Grants permission to get update the storage class of a specified image within a specified repository	Write	repository*		
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString
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 Registry Public

Amazon Elastic Container Registry Public (service prefix: `ecr-public`) 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 Public
- Resource types defined by Amazon Elastic Container Registry Public
- Condition keys for Amazon Elastic Container Registry Public

Actions defined by Amazon Elastic Container Registry Public

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCheckLayerAvailability	Grants permission to check the availability of multiple image layers in a specified registry and repository	Read	repository*		
BatchDeleteImage	Grants permission to delete a list of specified images within a specified repository	Write	repository*		
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*		
CreateRepository	Grants permission to create an image repository	Write	repository*		ecr-public:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRepository	Grants permission to delete an existing image repository	Write	repository*		
DeleteRepositoryPolicy	Grants permission to delete the repository policy from a specified repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageTags	Grants permission to describe all the image tags for a given repository	List	repository*		
DescribeImages	Grants permission to get metadata about the images in a repository, including image size, image tags, and creation date	Read	repository*		
DescribeRegistries	Grants permission to retrieve the catalog data associated with a registry	List	registry*		
DescribeRepositories	Grants permission to describe image repositories in a registry	List	repository		
GetAuthorizationToken	Grants permission to retrieve a token that is valid for a specified registry for 12 hours	Read			
GetRegistryCatalogData	Grants permission to retrieve the catalog data associated with a registry	Read	registry*		
GetRepositoryCatalogData	Grants permission to retrieve the catalog data associated with a repository	Read	repository*		
GetRepositoryPolicy	Grants permission to retrieve the repository policy for a specified repository	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InitiateLayerUpload	Grants permission to notify Amazon ECR that you intend to upload an image layer	Write	repository*		
ListTagsForResource	Grants permission to list the tags for an Amazon ECR resource	Read	repository*		
PutImage	Grants permission to create or update the image manifest associated with an image	Write	repository*		
PutRegistryCatalogData	Grants permission to create and update the catalog data associated with a registry	Write	registry*		
PutRepositoryCatalogData	Grants permission to update the catalog data associated with a repository	Write	repository*		
SetRepositoryPolicy	Grants permission to apply a repository policy on a specified repository to control access permissions	Permissions management	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	
UploadLayerPart	Grants permission to upload an image layer part to Amazon ECR Public	Write	repository*		

Resource types defined by Amazon Elastic Container Registry Public

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:${Partition}:ecr-public::${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		ecr-public:ResourceTag/${TagKey}
registry	arn:${Partition}:ecr-public::${Account}:registry/${RegistryId}	

Condition keys for Amazon Elastic Container Registry Public

Amazon Elastic Container Registry Public defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters create requests based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value associated with the resource	String
aws:TagKeys	Filters create requests based on the presence of mandatory tags in the request	ArrayOfString
ecr-public:ResourceTag/${TagKey}	Filters actions based on 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	capacity-provider*	aws:ResourceTag/${TagKey}	
				ecs:propagate-tags ecs:instance-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				metadata-tags-propagation aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Grants permission to create a new Amazon ECS cluster	Write	cluster*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:fargate-ephemeral-storage-kms-key	
CreateExpressGatewayService	Grants permission to create a new Amazon ECS Express Gateway service with cluster and task definition	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	ecs:RegisterTaskDefinition iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys ecs:task-definition ecs:subnet ecs:enable-ecs-managed-tags ecs:propagate-tags ecs:task-cpu ecs:task-memory	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
CreateTaskSet	Grants permission to create a new Amazon ECS task set	Write	task-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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/${TagKey}	
DeleteExpressGatewayService	Grants permission to delete a specified Express Gateway service	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteService	Grants permission to delete a specified service within a cluster	Write	service*		
				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/${TagKey} ecs:cluster	
DescribeExpressGatewayService	Grants permission to describe the specified Express Gateway service	Read	service*	ecs:cluster aws:ResourceTag/${TagKey}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServiceRevisions	Grants permission to describe one or more of your service revisions	Read	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-revision*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServices	Grants permission to describe the specified services running in your cluster	Read	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DescribeTasks	Grants permission to describe a specified task or tasks	Read	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccountSettings	Grants permission to list the account settings for an Amazon ECS resource for a specified principal	Read			
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServicesByNamespace	Grants permission to get a list of services that are running in a specified AWS Cloud Map Namespace	List		ecs:namespace	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTaskDefinitions	Grants permission to get a list of task definitions that are registered to your account	List			
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
PutSystemLogEvents	Grants permission to collect system logs from the container instances	Write	cluster*	aws:ResourceTag/${TagKey}	
			container-instance*	aws:ResourceTag/${TagKey} ecs:cluster 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:ResourceTag/${TagKey}	
				aws:RequestTag/${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		
			container-instance		
			service		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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		
			service		
			task		
			task-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			task-set		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCapacityProvider	Grants permission to update the specified capacity provider	Write	capacity-provider*		
				ecs:propagate-tags ecs:instance-metadata-tags-propagation aws:ResourceTag/${TagKey}	
UpdateCluster	Grants permission to modify the configuration or settings to use for a cluster	Write	cluster*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
UpdateContainerInstancesState	Grants permission to the user to modify the status of an Amazon ECS container instance	Write	container-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateExpressGatewayService	Grants permission to modify the parameters of an Express Gateway service	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	
				ecs:subnet ecs:enable-ecs-managed-tags ecs:propagate-tags ecs:task-cpu ecs:task-memory	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

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 AWS KMS key id provided in the request	String
ecs:instance-metadata-tags-propagation	Filters access by the instance metadata tags propagation setting of your Amazon ECS capacity provider	Bool
ecs:namespace	Filters access by the ARN of AWS 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

Condition keys	Description	Type
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 AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (service prefix: `drs`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elastic Disaster Recovery

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFailbackClientToRecoveryInstanceForDrs [permission only]	Grants permission to get associate failback client to recovery instance	Write	RecoveryInstanceResource*		
AssociateSourceNetworkStack	Grants permission to associate CloudFormation stack with source network	Write	SourceNetworkResource*		cloudformation:DescribeStackResource cloudformation:DescribeStacks drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchCreateVolumeSnapshotGroupForDrs [permission only]	Grants permission to batch create volume snapshot group	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteSnapshotRequestForDrs [permission only]	Grants permission to batch delete snapshot request	Write			
CreateConvertedSnapshotForDrs [permission only]	Grants permission to create converted snapshot	Write	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtendedSourceServer	Grants permission to extend a source server	Write		aws:RequestTag/${TagKey} aws:TagKeys	drs:DescribeSourceServers drs:GetReplicationConfiguration

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLaunchConfigurationTemplate	Grants permission to create launch configuration template	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryInstanceForDrs [permission only]	Grants permission to create recovery instance	Write	SourceServerResource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicationConfigurationTemplate	Grants permission to create replication configuration template	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey
CreateSourceNetwork	Grants permission to create a source network	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSourceServerForDrs [permission only]	Grants permission to create a source server	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJob	Grants permission to delete a job	Write	JobResource*		
DeleteLaunchAction	Grants permission to delete a launch action	Write	LaunchConfigurationTemplateResource		
			SourceServerResource		
DeleteLaunchConfigurationTemplate	Grants permission to delete launch configuration template	Write	LaunchConfigurationTemplateResource*		
DeleteRecoveryInstance	Grants permission to delete recovery instance	Write	RecoveryInstanceResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReplicationConfigurationTemplate	Grants permission to delete replication configuration template	Write	ReplicationConfigurationTemplateResource*		
DeleteSourceNetwork	Grants permission to delete source network	Write	SourceNetworkResource*		
DeleteSourceServer	Grants permission to delete source server	Write	SourceServerResource*		
DescribeJobLogItems	Grants permission to describe job log items	Read	JobResource*		
DescribeJobs	Grants permission to describe jobs	Read			
DescribeLaunchConfigurationTemplates	Grants permission to describe launch configuration template	Read			
DescribeRecoveryInstances	Grants permission to describe recovery instances	Read			drs:DescribeSourceServers ec2:DescribeInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRecoverySnapshots	Grants permission to describe recovery snapshots	Read	SourceServerResource*		
DescribeReplicationConfigurationTemplates	Grants permission to describe replication configuration template	Read			
DescribeReplicationServerAssociationsForDrs [permission only]	Grants permission to describe replication server associations	Read			
DescribeSnapshotRequestsForDrs [permission only]	Grants permission to describe snapshot requests	Read			
DescribeSourceNetworks	Grants permission to describe source networks	Read			
DescribeSourceServers	Grants permission to describe source servers	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisconnectRecoveryInstance	Grants permission to disconnect recovery instance	Write	RecoveryInstanceResource*		
DisconnectSourceServer	Grants permission to disconnect source server	Write	SourceServerResource*		
ExportSourceNetworkCfnTemplate	Grants permission to export CloudFormation template which contains source network resources	Write	SourceNetworkResource*		s3:GetBucketLocation s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
GetAgentCommandForDrs [permission only]	Grants permission to get agent command	Read	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAgentConfirmedResumeInfoForDrs [permission only]	Grants permission to get agent confirmed resume info	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentInstallationAssetsForDrs [permission only]	Grants permission to get agent installation assets	Read			
GetAgentReplicationInfoForDrs [permission only]	Grants permission to get agent replication info	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetAgentRuntimeConfigurationForDrs [permission only]	Grants permission to get agent runtime configuration	Read	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAgentSnapshotCreditsForDrs [permission only]	Grants permission to get agent snapshot credits	Read	RecoveryInstanceResource*		
			SourceServerResource*		
GetChannelCommandsForDrs [permission only]	Grants permission to get channel commands	Read			
GetFailbackCommandForDrs [permission only]	Grants permission to get failback command	Read	RecoveryInstanceResource*		
GetFailbackLaunchRequestedForDrs [permission only]	Grants permission to get failback launch requested	Read	RecoveryInstanceResource*		
GetFailbackReplicationConfiguration	Grants permission to get failback replication configuration	Read	RecoveryInstanceResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLaunchConfiguration	Grants permission to get launch configuration	Read	SourceServerResource*		
GetReplicationConfiguration	Grants permission to get replication configuration	Read	SourceServerResource*		
GetSuggestedFailbackClientDeviceMappingForDrs [permission only]	Grants permission to get suggested failback client device mapping	Read	RecoveryInstanceResource*		
InitializeService	Grants permission to initialize service	Write			iam:AddRoleToInstanceProfile iam:CreateInstanceProfile iam:CreateServiceLinkedRole iam:GetInstanceProfile

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
IssueAgentCertificateForDrs [permission only]	Grants permission to issue an agent certificate	Write	RecoveryInstanceResource*		
			SourceServerResource*		
ListExtensibleSourceServers	Grants permission to list extensible source servers	Read			drs:DescribeSourceServers
ListLaunchActions	Grants permission to list launch actions	Read	LaunchConfigurationTemplateResource		
			SourceServerResource		
ListStagingAccounts	Grants permission to list staging accounts	Read			
ListTagsForResource	Grants permission to list tags for a resource	Read			
NotifyAgentAuthenticationForDrs [permission only]	Grants permission to notify agent authentication	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyAgentConnectedForDrs [permission only]	Grants permission to notify agent is connected	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentDisconnectedForDrs [permission only]	Grants permission to notify agent is disconnected	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyAgentReplicationProgressForDrs [permission only]	Grants permission to notify agent replication progress	Write	RecoveryInstanceResource*		
			SourceServerResource*		
NotifyConsistencyAttainedForDrs [permission only]	Grants permission to notify consistency attained	Write	RecoveryInstanceResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyReplicationServerAuthenticationForDrs [permission only]	Grants permission to notify replication server authentication	Write	RecoveryInstanceResource*		
NotifyVolumeEventForDrs [permission only]	Grants permission to notify replicator volume events	Write	SourceServerResource*		
PutLaunchAction	Grants permission to put a launch action	Write	LaunchConfigurationTemplateResource		ssm:DescribeDocument
			SourceServerResource		
RetryDataReplication	Grants permission to retry data replication	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReverseReplication	Grants permission to reverse replication	Write	RecoveryInstanceResource*		drs:DescribeReplicationConfigurationTemplates drs:DescribeSourceServers ec2:DescribeInstances
				aws:RequestTag/${TagKey} aws:TagKeys	
SendAgentLogsForDrs [permission only]	Grants permission to send agent logs	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendAgentMetricsForDrs [permission only]	Grants permission to send agent metrics	Write	RecoveryInstanceResource*		
			SourceServerResource*		
SendChannelCommandResultForDrs [permission only]	Grants permission to send channel command result	Write			
SendClientLogsForDrs [permission only]	Grants permission to send client logs	Write			
SendClientMetricsForDrs [permission only]	Grants permission to send client metrics	Write			
SendVolumeStatsForDrs [permission only]	Grants permission to send volume throughput statistics	Write	SourceServerResource*		
StartFailbackLaunch	Grants permission to start failback launch	Write	RecoveryInstanceResource*		

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
StartRecovery	Grants permission to start recovery	Write	SourceServerResource*		drs:CreateRecoveryInstanceForDrs drs:ListTagsForResource ec2:AttachVolume ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateSnapshot

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:CreateTags ec2:CreateVolume ec2:DeleteLaunchTemplateVersions ec2:DeleteSnapshot ec2:DeleteVolume ec2:DescribeAccountAttributes ec2:DescribeAvailabilityZones ec2:DescribeImages ec2:DescribeInstanceAttribute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSnapshots ec2:DescribeSubnets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeVolumes ec2:DetachVolume ec2:ModifyInstanceAttribute ec2:ModifyLaunchTemplate ec2:RevokeSecurityGroupEgress ec2:RunInstances ec2:StartInstances ec2:StopInstances ec2:TerminateInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
StartReplication	Grants permission to start replication	Write	SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSourceNetworkRecovery	Grants permission to start network recovery	Write	SourceNetworkResource*		cloudformation:CreateStack cloudformation:DescribeStackResource cloudformation:DescribeStacks cloudformation:UpdateStack drs:GetLaunchConfiguration ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunch

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					Templates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyLaunchTemplate s3:GetObject s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	
StartSourceNetworkReplication	Grants permission to start network replication	Write	SourceNetworkResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopFailback	Grants permission to stop failback	Write	RecoveryInstanceResource*		
StopReplication	Grants permission to stop replication	Write	SourceServerResource*		
StopSourceNetworkReplication	Grants permission to stop network replication	Write	SourceNetworkResource*		
TagResource	Grants permission to assign a resource tag	Tagging	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SourceServerResource		
				aws:RequestTag/${TagKey} aws:TagKeys drs:CreateAction	
TerminateRecoveryInstances	Grants permission to terminate recovery instances	Write	RecoveryInstanceResource*		drs:DescribeSourceServers ec2:DeleteVolume ec2:DescribeInstances ec2:DescribeVolumes ec2:TerminateInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	JobResource		
			LaunchConfigurationTemplateResource		
			RecoveryInstanceResource		
			ReplicationConfigurationTemplateResource		
			SourceNetworkResource		
			SourceServerResource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAgentBacklogForDrs [permission only]	Grants permission to update agent backlog	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentConversionInfoForDrs [permission only]	Grants permission to update agent conversion info	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentReplicationInfoForDrs [permission only]	Grants permission to update agent replication info	Write	RecoveryInstanceResource*		
			SourceServerResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgentReplicationProcessStateForDrs [permission only]	Grants permission to update agent replication process state	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateAgentSourcePropertiesForDrs [permission only]	Grants permission to update agent source properties	Write	RecoveryInstanceResource*		
			SourceServerResource*		
UpdateFailbackClientDeviceMappingForDrs [permission only]	Grants permission to update failback client device mapping	Write	RecoveryInstanceResource*		
UpdateFailbackClientLastSeenForDrs [permission only]	Grants permission to update failback client last seen	Write	RecoveryInstanceResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFailbackReplicationConfiguration	Grants permission to update failback replication configuration	Write	RecoveryInstanceResource*		
UpdateLaunchConfiguration	Grants permission to update launch configuration	Write	SourceServerResource*		ec2:DescribeInstances
UpdateLaunchConfigurationTemplate	Grants permission to update launch configuration	Write	LaunchConfigurationTemplateResource*		
UpdateReplicationCertificateForDrs [permission only]	Grants permission to update a replication certificate	Write	RecoveryInstanceResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateReplicationConfiguration	Grants permission to update replication configuration	Write	SourceServerResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateReplicationConfigurationTemplate	Grants permission to update replication configuration template	Write	ReplicationConfigurationTemplateResource*		ec2:CreateSecurityGroup ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetEbsDefaultKmsKeyId ec2:GetEbsEncryptionByDefault kms:CreateGrant kms:DescribeKey

Resource types defined by AWS Elastic Disaster Recovery

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
JobResource	`arn:${Partition}:drs:${Region}:${Account}:job/${JobID}`	aws:ResourceTag/${TagKey}
RecoveryInstanceResource	`arn:${Partition}:drs:${Region}:${Account}:recovery-instance/${RecoveryInstanceID}`	aws:ResourceTag/${TagKey} drs:EC2InstanceARN
ReplicationConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:replication-configuration-template/${ReplicationConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
LaunchConfigurationTemplateResource	`arn:${Partition}:drs:${Region}:${Account}:launch-configuration-template/${LaunchConfigurationTemplateID}`	aws:ResourceTag/${TagKey}
SourceServerResource	`arn:${Partition}:drs:${Region}:${Account}:source-server/${SourceServerID}`	aws:ResourceTag/${TagKey}
SourceNetworkResource	`arn:${Partition}:drs:${Region}:${Account}:source-network/${SourceNetworkID}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
drs:CreateAction	Filters access by the name of a resource-creating API action	String
drs:EC2InstanceARN	Filters access by the EC2 instance the request originated from	ARN

Actions, resources, and condition keys for Amazon Elastic File System

Amazon Elastic File System (service prefix: `elasticfilesystem`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic File System
- Resource types defined by Amazon Elastic File System

- Condition keys for Amazon Elastic File System

Actions defined by Amazon Elastic File System

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Backup [permission only]	Grants permission to start a backup job for an existing file system	Write	file-system*		
ClientMount [permission only]	Grants permission to allow an NFS client read-access to a file system	Read	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientRootAccess [permission only]	Grants permission to allow an NFS client root-access to a file system	Write	file-system*		
				elasticfilesystem:	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
CreateAccessPoint	Grants permission to create an access point for the specified file system	Write	file-system*		elasticfilesystem:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
CreateTags	Grants permission to create or overwrite tags associated with a file system; deprecated, see TagResource	Tagging	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account in the AWS region of the endpoint that is being called	List	file-system		
DescribeLifecycleConfiguration	Grants permission to view the LifecycleConfiguration object for an Amazon EFS file system	Read	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account in the AWS region of the endpoint that is being called	List	file-system		
DescribeTags	Grants permission to view the tags associated with a file system	Read	file-system*		
ListTagsForResource	Grants permission to view the tags associated with the specified Amazon EFS resource	Read	access-point		
			file-system		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Backup by creating a new BackupPolicy object	Write	file-system*		
PutFileSystemPolicy	Grants permission to apply a resource-level policy that defines the actions allowed or denied from given actors for the specified file system	Permissions management	file-system*		
PutLifecycleConfiguration	Grants permission to enable lifecycle management by creating a new Lifecycle Configuration object	Write	file-system*		
ReplicationRead [permission only]	Grants permission to read file system data for replication	Read	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
UntagResource	Grants permission to delete the specified tags from an Amazon EFS resource	Tagging	access-point		
			file-system		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
elasticfilesystem:AccessPointArn	Filters access by the ARN of the access point used to mount the file system	ARN
elasticfilesystem:AccessedViaMountTarget	Filters access by whether the file system is accessed via mount targets	Bool
elasticfilesystem:CreateAction	Filters access by the name of a resource-creating API action	String
elasticfilesystem:Encrypted	Filters access by whether users can create only encrypted or unencrypted file systems	Bool

Actions, resources, and condition keys for Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (service prefix: `eks`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by Amazon Elastic Kubernetes Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessKubernetesApi [permission only]	Grants permission to view Kubernetes objects via AWS EKS console	Read	cluster*		
AssociateAccessPolicy	Grants permission to associate an Amazon EKS access policy to an Amazon EKS access entry	Write	access-entry*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 eks:issuerUrl	
CreateAccessEntry	Grants permission to create an Amazon EKS access entry	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Grants permission to create an Amazon EKS add-on	Write	cluster*		
			podidentityassociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCapability	Grants permission to create a capability for an Amazon EKS cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create an Amazon EKS cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:blockStorageEnabled eks:loggingType/${type}	
CreateEksAnywhereSubscription	Grants permission to create an EKS Anywhere subscription	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Grants permission to create an AWS Fargate profile	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Grants permission to create an Amazon EKS Nodegroup	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	Grants permission to create an EKS Pod Identity association	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Grants permission to delete an Amazon EKS access entry	Write	access-entry*		
DeleteAddon	Grants permission to delete an Amazon EKS add-on	Write	addon*		
			podidentityassociation		
DeleteCapability	Grants permission to delete a capability from an Amazon EKS cluster	Write	capability*		
DeleteCluster	Grants permission to delete an Amazon EKS cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEksAnywhereSubscription	Grants permission to describe an EKS Anywhere subscription	Write	eks-anywhere-subscription*		
DeleteFargateProfile	Grants permission to delete an AWS Fargate profile	Write	fargateprofile*		
DeleteNodegroup	Grants permission to delete an Amazon EKS Nodegroup	Write	nodegroup*		
DeletePodIdentityAssociation	Grants permission to delete an EKS Pod Identity association	Write	podidentityassociation*		
DeregisterCluster	Grants permission to deregister an External cluster	Write	cluster*		
DescribeAccessEntry	Grants permission to describe an Amazon EKS access entry	Read	access-entry*		
DescribeAddon	Grants permission to retrieve descriptive information about an Amazon EKS add-on	Read	addon*		
DescribeAddonConfiguration	Grants permission to list configuration options about an Amazon EKS add-on	Read			
DescribeAddonVersions	Grants permission to retrieve descriptive version information about the add-ons that Amazon EKS Add-ons supports	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapability	Grants permission to describe a capability for an Amazon EKS cluster	Read	capability*		
DescribeCluster	Grants permission to retrieve descriptive information about an Amazon EKS cluster	Read	cluster*		
DescribeClusterVersions	Grants permission to retrieve descriptive information about Kubernetes versions that Amazon EKS clusters support	Read			
DescribeEksAnywhereSubscription	Grants permission to describe an EKS Anywhere subscription	Read	eks-anywhere-subscription*		
DescribeFargateProfile	Grants permission to retrieve descriptive information about an AWS Fargate profile associated with a cluster	Read	fargateprofile*		
DescribeIdentityProviderConfig	Grants permission to retrieve descriptive information about an Idp config associated with a cluster	Read	identityproviderconfig*		
DescribeInsight	Grants permission to retrieve descriptive information of a detected insight for a specified cluster	Read	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInsightsRefresh	Grants permission to retrieve the status of the latest on-demand cluster insights refresh operation	Read	cluster*		
DescribeNodegroup	Grants permission to retrieve descriptive information about an Amazon EKS nodegroup	Read	nodegroup*		
DescribePodIdentityAssociation	Grants permission to describe an EKS Pod Identity association	Read	podidentityassociation*		
DescribeUpdate	Grants permission to retrieve a given update for a given Amazon EKS cluster/nodegroup/add-on (in the specified or default region)	Read	cluster*		
			addon		
			capability		
			nodegroup		
DisassociateAccessPolicy	Grants permission to disassociate an Amazon EKS access policy from an Amazon EKS acces entry	Write	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIdentityProviderConfig	Grants permission to delete an asssociated Idp config	Write	identityproviderconfig*		
ListAccessEntries	Grants permission to list all Amazon EKS access entries	List	cluster*		
ListAccessPolicies	Grants permission to list Amazon EKS access policies	List			
ListAddons	Grants permission to list the Amazon EKS add-ons in your AWS account (in the specified or default region) for a given cluster	List	cluster*		
ListAssociatedAccessPolicies	Grants permission to list associated access policy on and Amazon EKS access entry	List	access-entry*		
ListCapabilities	Grants permission to list capabilities for an Amazon EKS cluster	List	cluster*		
ListClusters	Grants permission to list the Amazon EKS clusters in your AWS account (in the specified or default region)	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDashboardData	Grants permission to list dashboard data. The Amazon EKS Dashboard aggregates information about cluster resources across multiple accounts and regions. The dashboard includes information about EC2 Instances and EKS Cluster versions	Read	dashboard*		
ListDashboardResources	Grants permission to list dashboard resources. The Amazon EKS Dashboard aggregates information about cluster resources across multiple accounts and regions. The dashboard includes information about EC2 Instances and EKS Cluster versions	Read	dashboard*		
ListEksAnywhereSubscriptions	Grants permission to list EKS Anywhere subscriptions	List			
ListFargateProfiles	Grants permission to list the AWS Fargate profiles in your AWS account (in the specified or default region) associated with a given cluster	List	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIdentityProviderConfigs	Grants permission to list the Idp configs in your AWS account (in the specified or default region) associated with a given cluster	List	cluster*		
ListInsights	Grants permission to list all detected insights for a specified cluster	List	cluster*		
ListNodegroups	Grants permission to list the Amazon EKS nodegroups in your AWS account (in the specified or default region) attached to given cluster	List	cluster*		
ListPodIdentityAssociations	Grants permission to list EKS Pod Identity associations	List	cluster*		
ListTagsForResource	Grants permission to list tags for the specified resource	Read	addon		
			capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fargateprofile		
			identityproviderconfig		
			nodegroup		
ListUpdates	Grants permission to list the updates for a given Amazon EKS cluster/nodegroup/add-on (in the specified or default region)	List	cluster*		
			addon		
			capability		
			nodegroup		
MutateViaKubernetesApi [permission only]	Grants permission to modify Kubernetes objects via AWS console	Write	cluster*		eks:AccessKubernetesApi
RegisterCluster	Grants permission to register an External cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInsightsRefresh	Grants permission to initiate an on-demand refresh operation for cluster insights, getting the latest analysis outside of the standard refresh schedule	Write	cluster*		
TagResource	Grants permission to tag the specified resource	Tagging	access-entry		
			addon		
			capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag the specified resource	Tagging	access-entry		
			addon		
			capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	Grants permission to update an Amazon EKS access entry	Write	access-entry*		
UpdateAddon	Grants permission to update Amazon EKS add-on configurations, such as the VPC-CNI version	Write	addon*		
			podidentityassociation		
UpdateCapability	Grants permission to update a capability for an Amazon EKS cluster	Write	capability*		
UpdateClusterConfig	Grants permission to update Amazon EKS cluster configurations (eg: API server endpoint access)	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled eks:loggingType/${type}	
UpdateClusterVersion	Grants permission to update the Kubernetes version of an Amazon EKS cluster	Write	cluster*		
UpdateEksAnywhereSubscription	Grants permission to update an EKS Anywhere subscription	Write	eks-anywhere-subscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNodegroupConfig	Grants permission to update Amazon EKS nodegroup configurations (eg: min/max/desired capacity or labels)	Write	nodegroup*		
UpdateNodegroupVersion	Grants permission to update the Kubernetes version of an Amazon EKS nodegroup	Write	nodegroup*		
UpdatePodIdentityAssociation	Grants permission to update an EKS Pod Identity association	Write	podidentityassociation*		

Resource types defined by Amazon Elastic Kubernetes Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}
nodegroup	`arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${ClusterName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	aws:ResourceTag/${TagKey}
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName eks:kubernetesGroups eks:principalArn eks:username

Resource types	ARN	Condition keys
access-policy	arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}	
dashboard	arn:${Partition}:eks:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}
capability	arn:${Partition}:eks:${Region}:${Account}:capability/${ClusterName}/${CapabilityType}/${CapabilityName}/${UUID}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the EKS service	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String
aws:TagKeys	Filters access by the list of all the tag key names present in the request the user makes to the EKS service	ArrayOfString
eks:accessEntryType	Filters access by the access entry type present in the access entry requests the user makes to the EKS service	String

Condition keys	Description	Type
eks:accessScope	Filters access by the accessScope present in the associate / disassociate access policy requests the user makes to the EKS service	String
eks:authenticationMode	Filters access by the authenticationMode present in the create / update cluster request	String
eks:blockStorageEnabled	Filters access by the block storage enabled parameter in the create / update cluster request	Bool
eks:bootstrapClusterCreatorAdminPermissions	Filters access by the bootstrapClusterCreatorAdminPermissions present in the create cluster request	Bool
eks:bootstrapSelfManagedAddons	Filters access by the bootstrapSelfManagedAddons present in the create cluster request	Bool
eks:clientId	Filters access by the clientId present in the associate IdentityProviderConfig request the user makes to the EKS service	String
eks:clusterName	Filters access by the clusterName present in the access entry requests the user makes to the EKS service	String
eks:computeConfigEnabled	Filters access by the compute config enabled parameter in the create / update cluster request	Bool
eks:elasticLoadBalancingEnabled	Filters access by the elastic load balancing enabled parameter in the create / update cluster request	Bool
eks:issuerUrl	Filters access by the issuerUrl present in the associate IdentityProviderConfig request the user makes to the EKS service	String

Condition keys	Description	Type
eks:kubernetesGroups	Filters access by the kubernetesGroups present in the access entry requests the user makes to the EKS service	ArrayOfString
eks:loggingType/${type}	Filters access by the cluster logging enabled and type parameter in the create / update cluster request	Bool
eks:namespaces	Filters access by the namespaces present in the associate / disassociate access policy requests the user makes to the EKS service	ArrayOfString
eks:policyArn	Filters access by the policyArn present in the access entry requests the user makes to the EKS service	ARN
eks:principalArn	Filters access by the principalArn present in the access entry requests requests the user makes to the EKS service	ARN
eks:supportType	Filters access by the supportType present in the create / update cluster request	String
eks:username	Filters access by the Kubernetes username present in the access entry requests the user makes to the EKS service	String

Actions, resources, and condition keys for AWS Elastic Load Balancing

AWS Elastic Load Balancing (service prefix: `elasticloadbalancing`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elastic Load Balancing

- Resource types defined by AWS Elastic Load Balancing
- Condition keys for AWS Elastic Load Balancing

Actions defined by AWS Elastic Load Balancing

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTags	Grants permission to add the specified tags to the specified load balancer. Each load balancer can have a maximum of 10 tags	Tagging	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Grants permission to associate one or more security groups with your load balancer in a virtual private cloud (VPC)	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	Grants permission to add one or more subnets to the set of configured subnets for the specified load balancer	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
Configure HealthCheck	Grants permission to specify the health check settings to use when evaluating the health state of your back-end instances	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppCookieStickinessPolicy	Grants permission to generate a stickiness policy with sticky session lifetimes that follow that of an application-generated cookie	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLBCookieStickinessPolicy	Grants permission to generate a stickiness policy with sticky session lifetimes controlled by the lifetime of the browser (user-agent) or a specified expiration period	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoadBalancer	Grants permission to create a load balancer	Write	loadbalancer		elasticloadbalancing:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerListeners	Grants permission to create one or more listeners for the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	Grants permission to create a policy with the specified attributes for the specified load balancer	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	Grants permission to delete the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLoadBalancerListeners	Grants permission to delete the specified listeners from the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	Grants permission to delete the specified policy from the specified load balancer. This policy must not be enabled for any listeners	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterInstancesFromLoadBalancer	Grants permission to deregister the specified instances from the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	Grants permission to describe the state of the specified instances with respect to the specified load balancer	Read			
DescribeLoadBalancerAttributes	Grants permission to describe the attributes for the specified load balancer	Read			
DescribeLoadBalancerPolicies	Grants permission to describe the specified policies	Read			
DescribeLoadBalancerPolicyTypes	Grants permission to describe the specified load balancer policy types	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLoadBalancers	Grants permission to describe the specified the load balancers. If no load balancers are specified, the call describes all of your load balancers	List			
DescribeTags	Grants permission to describe the tags associated with the specified load balancers	Read			
DetachLoadBalancerFromSubnets	Grants permission to remove the specified subnets from the set of configured subnets for the load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableAvailabilityZonesForLoadBalancer	Grants permission to remove the specified Availability Zones from the set of Availability Zones for the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	Grants permission to add the specified Availability Zones to the set of Availability Zones for the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Grants permission to modify the attributes of the specified load balancer	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	Grants permission to add the specified instances to the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Grants permission to remove one or more tags from the specified load balancer	Tagging	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerListenerSSLCertificate	Grants permission to set the certificate that terminates the specified listener's SSL connections	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesForBackendServer	Grants permission to replace the set of policies associated with the specified port on which the back-end server is listening with a new set of policies	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLoadBalancerPoliciesOfListener	Grants permission to replace the current set of policies for the specified load balancer port with the specified set of policies	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Resource types defined by AWS Elastic Load Balancing

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Condition keys for AWS Elastic Load Balancing

AWS Elastic Load Balancing defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
elasticloadbalancing:CreateAction	Filters access by the name of a resource-creating API action	String
elasticloadbalanci	Filters access by the listener protocols that are allowed in the request	ArrayOfString

Condition keys	Description	Type
ng:ListenerProtocol		
elasticloadbalancing:ResourceTag/	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
elasticloadbalancing:ResourceTag/${TagKey}	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
elasticloadbalancing:Scheme	Filters access by the load balancer scheme that are allowed in the request	String
elasticloadbalancing:SecurityGroup	Filters access by the security-group IDs that are allowed in the request	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filters access by the SSL Security Policies that are allowed in the request	ArrayOfString
elasticloadbalancing:Subnet	Filters access by the subnet IDs that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 (service prefix: `elasticloadbalancing`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elastic Load Balancing V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddListenerCertificates	Grants permission to add the specified certificates to the specified secure listener	Write	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:Resour	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ceTag/${TagKey}	
AddTags	Grants permission to add the specified tags to the specified load balancer. Each load balancer can have a maximum of 10 tags	Tagging	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
AddTrustStoreRevocations	Grants permission to add revocations to a trust store	Write	truststore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for load balancers	Permissions management			
CreateListener	Grants permission to create a listener for the specified Application Load Balancer	Write	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoadBalancer	Grants permission to create a load balancer	Write	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRule	Grants permission to create a rule for the specified listener	Write	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	Grants permission to create a target group	Write	targetgroup*		elasticloadbalancing:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	Grants permission to create a trust store	Write	truststore		elasticloadbalancing:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateWebACLAssociation [permission only]	Grants permission to associate WAF WebACL to the specified load balancer	Write	loadbalancer/app/*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	Grants permission to delete the specified listener	Write	listener/app*		
			listener/gwy*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLoadBalancer	Grants permission to delete the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteRule	Grants permission to delete the specified rule	Write	listener-rule/app*		
			listener-rule/net*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}	
DeleteTargetGroup	Grants permission to delete the specified target group	Write	targetgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	Grants permission to delete the specified trust store	Write	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteWebACLAssociation [permission only]	Grants permission to disassociate WAF WebACL from the specified load balancer	Write	loadbalancer/app/*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeregisterTargets	Grants permission to deregister the specified targets from the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	Grants permission to describe the Elastic Load Balancing resource limits for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeListeners	Grants permission to describe the specified listeners or the listeners for the specified Application Load Balancer	Read			
DescribeLoadBalancerAttributes	Grants permission to describe the attributes for the specified load balancer	Read			
DescribeLoadBalancers	Grants permission to describe the specified the load balancers. If no load balancers are specified, the call describes all of your load balancers	List			
DescribeRules	Grants permission to describe the specified rules or the rules for the specified listener	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTrustStores	Grants permission to describe the specified trust stores or all of your trust stores	Read			
DescribeWebACLAssociation [permission only]	Grants permission to describe all load balancers associated to a WAF WebACL in your account	List			
GetLoadBalancerWebACL [permission only]	Grants permission to retrieve the WAF WebACL associated to the specified load balancer	Read	loadbalancer/app/*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetResourcePolicy	Grants permission to retrieve the resource policy associated with the resource	Read	truststore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreCaCertificatesBundle	Grants permission to retrieve a trust store CA certificates bundle	Read	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreRevocationContent	Grants permission to retrieve a trust store revocation content	Read	truststore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	Grants permission to modify the capacity reservation for a load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpPools	Grants permission to modify the ip pools for a load balancer	Write	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	Grants permission to modify the specified properties of the specified listener	Write	listener/app*		
			listener/gwy*		
			listener/net*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyListenerAttributes	Grants permission to modify the attributes of the specified listener	Write	listener/app*		
			listener/gwy*		
			listener/net*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Grants permission to modify the attributes of the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyRule	Grants permission to modify the specified rule	Write	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	Grants permission to modify the health checks used when evaluating the health state of the targets in the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTargetGroupAttributes	Grants permission to modify the specified attributes of the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	Grants permission to modify the specified trust store	Write	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	Grants permission to register the specified targets with the specified target group	Write	targetgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	Grants permission to remove the specified certificates of the specified secure listener	Write	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Grants permission to remove one or more tags from the specified load balancer	Tagging	listener-rule/app		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	Grants permission to remove revocations from a trust store	Write	truststore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetIpAddressType	Grants permission to set the type of IP addresses used by the subnets of the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetRulePriorities	Grants permission to set the priorities of the specified rules	Write	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	Grants permission to associate the specified security groups with the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	Grants permission to enable the Availability Zone for the specified subnets for the specified load balancer	Write	loadbalancer/app/		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [permission only]	Grants permission to give WebAcl permission to WAF	Write			

Resource types defined by AWS Elastic Load Balancing V2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
listener/gwy	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/gwy/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
loadbalancer/gwy/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/gwy/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/net/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
targetgroup	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:targetgroup/${TargetGroupName}/${TargetGroupId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
truststore	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:truststore/${TrustStoreName}/${TrustStoreId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Condition keys for AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
elasticloadbalancing:CreateAction	Filters access by the name of a resource-creating API action	String
elasticloadbalancing:ListenerProtocol	Filters access by the listener protocol that is allowed in the request	String
elasticloadbalancing:ResourceTag/${TagKey}	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
elasticloadbalancing:Scheme	Filters access by the load balancer scheme that is allowed in the request	String

Condition keys	Description	Type
elasticloadbalancing:SecurityGroup	Filters access by the security-group IDs that are allowed in the request	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filters access by the SSL Security Policies that are allowed in the request	ArrayOfString
elasticloadbalancing:Subnet	Filters access by the subnet IDs that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Elastic MapReduce

Amazon Elastic MapReduce (service prefix: `elasticmapreduce`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic MapReduce
- Resource types defined by Amazon Elastic MapReduce
- Condition keys for Amazon Elastic MapReduce

Actions defined by Amazon Elastic MapReduce

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

The DescribeJobFlows API is deprecated and will eventually be removed. We recommend you use ListClusters, DescribeCluster, ListSteps, ListInstanceGroups and ListBootstrapActions instead

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessAllEventLogs	Grants permission to view all event logs in a persistent application history server	Write	cluster*		
AddInstanceFleet	Grants permission to add an instance fleet to a running cluster	Write	cluster*		
AddInstanceGroups	Grants permission to add instance groups to a running cluster	Write	cluster*		
AddJobFlowSteps	Grants permission to add new steps to a running cluster	Write	cluster*		
				elasticmapreduce:ExecutionRoleArn	
AddTags	Grants permission to add tags to an Amazon EMR resource	Tagging	cluster		
			editor		
			notebook-execution		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [permission only]	Grants permission to attach an EMR notebook to a compute engine	Write	editor*		
CancelSteps	Grants permission to cancel a pending step or steps in a running cluster	Write	cluster*		
CreateEditor [permission only]	Grants permission to create an EMR notebook	Write	cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	Grants permission to create a persistent application history server	Write	cluster*		
CreateRepository [permission only]	Grants permission to create an EMR notebook repository	Write			
CreateSecurityConfiguration	Grants permission to create a security configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStudio	Grants permission to create an EMR Studio	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	Grants permission to launch an EMR Studio using IAM authentication mode	Write	studio*		
CreateStudioSessionMapping	Grants permission to create an EMR Studio session mapping	Write	studio*		
DeleteEditor [permission only]	Grants permission to delete an EMR notebook	Write	editor*		
DeleteRepository [permission only]	Grants permission to delete an EMR notebook repository	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSecurityConfiguration	Grants permission to delete a security configuration	Write			
DeleteStudio	Grants permission to delete an EMR Studio	Write	studio*		
DeleteStudioSessionMapping	Grants permission to delete an EMR Studio session mapping	Write	studio*		
DeleteWorkspaceAccess [permission only]	Grants permission to block an identity from opening a collaborative workspace	Permissions management	editor*		
DescribeCluster	Grants permission to get details about a cluster, including status, hardware and software configuration, VPC settings, and so on	Read	cluster*		
DescribeEditor [permission only]	Grants permission to view information about a notebook, including status, user, role, tags, location, and more	Read	editor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJobFlows	Grants permission to describe details of clusters (job flows). This API is deprecated and will eventually be removed. We recommend you use ListClusters, DescribeCluster, ListSteps, ListInstanceGroups and ListBootstrapActions instead	Read	cluster*		
DescribeNotebookExecution	Grants permission to view information about a notebook execution	Read	notebook-execution*		
DescribePersistentAppUI	Grants permission to describe a persistent application history server	Read	cluster*		
DescribeReleaseLabel	Grants permission to view information about an EMR release, such as which applications are supported	Read			
DescribeRepository [permission only]	Grants permission to describe an EMR notebook repository	Read			
DescribeSecurityConfiguration	Grants permission to get details of a security configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStep	Grants permission to get details about a cluster step	Read	cluster*		
DescribeStudio	Grants permission to view information about an EMR Studio	Read	studio*		
DetachEditor [permission only]	Grants permission to detach an EMR notebook from a compute engine	Write	editor*		
GetAutoTerminationPolicy	Grants permission to retrieve the auto-termination policy associated with a cluster	Read	cluster*		
GetBlockPublicAccessConfiguration	Grants permission to retrieve the EMR block public access configuration for the AWS account in the Region	Read			
GetClusterSessionCredentials	Grants permission to retrieve HTTP basic credentials associated with a given execution IAM Role for a fine-grained access control enabled EMR Cluster	Write	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	Grants permission to retrieve the managed scaling policy associated with a cluster	Read	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOnClusterAppUIPresignedURL	Grants permission to get a presigned URL for an application history server running on the cluster	Write	cluster*		
GetPersistentAppUIPresignedURL	Grants permission to get a presigned URL for a persistent application history server	Write	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	Grants permission to view information about an EMR Studio session mapping	Read	studio*		
LinkRepository [permission only]	Grants permission to link an EMR notebook repository to EMR notebooks	Write			
ListBootstrapActions	Grants permission to get details about the bootstrap actions associated with a cluster	Read	cluster*		
ListClusters	Grants permission to get the status of accessible clusters	List			
ListEditors [permission only]	Grants permission to list summary information for accessible EMR notebooks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstanceFleets	Grants permission to get details of instance fleets in a cluster	Read	cluster*		
ListInstanceGroups	Grants permission to get details of instance groups in a cluster	Read	cluster*		
ListInstances	Grants permission to get details about the Amazon EC2 instances in a cluster	Read	cluster*		
ListNotebookExecutions	Grants permission to list summary information for notebook executions	List			
ListReleaseLabels	Grants permission to list and filter the available EMR releases in the current region	List			
ListRepositories [permission only]	Grants permission to list existing EMR notebook repositories	List			
ListSecurityConfigurations	Grants permission to list available security configurations in this account by name, along with creation dates and times	List			
ListSteps	Grants permission to list steps associated with a cluster	Read	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStudioSessionMappings	Grants permission to list summary information about EMR Studio session mappings	List			
ListStudios	Grants permission to list summary information about EMR Studios	List			
ListSupportedInstanceTypes	Grants permission to list the Amazon EC2 instance types that an Amazon EMR release supports	List			
ListWorkspaceAccessIdentities [permission only]	Grants permission to list identities that are granted access to a workspace	List	editor*		
ModifyCluster	Grants permission to change cluster settings such as number of steps that can be executed concurrently for a cluster	Write	cluster*		
ModifyInstanceFleet	Grants permission to change the target On-Demand and target Spot capacities for a instance fleet	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceGroups	Grants permission to change the number and configuration of EC2 instances for an instance group	Write	cluster		
OpenEditorInConsole [permission only]	Grants permission to launch the Jupyter notebook editor for an EMR notebook from within the console	Write	editor*		
			cluster		
PutAutoScalingPolicy	Grants permission to create or update an automatic scaling policy for a core instance group or task instance group	Write	cluster*		
PutAutoTerminationPolicy	Grants permission to create or update the auto-termination policy associated with a cluster	Write	cluster*		
PutBlockPublicAccessConfiguration	Grants permission to create or update the EMR block public access configuration for the AWS account in the Region	Permissions management			
PutManagedScalingPolicy	Grants permission to create or update the managed scaling policy associated with a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutWorkspaceAccess [permission only]	Grants permission to allow an identity to open a collaborative workspace	Permissions management	editor*		
RemoveAutoScalingPolicy	Grants permission to remove an automatic scaling policy from an instance group	Write	cluster*		
RemoveAutoTerminationPolicy	Grants permission to remove the auto-termination policy associated with a cluster	Write	cluster*		
RemoveManagedScalingPolicy	Grants permission to remove the managed scaling policy associated with a cluster	Write	cluster*		
RemoveTags	Grants permission to remove tags from an Amazon EMR resource	Tagging	cluster		
			editor		
			notebook-execution		
			studio		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RunJobFlow	Grants permission to create and launch a cluster (job flow)	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	Grants permission to add and remove auto terminate after step execution for a cluster	Write	cluster*		
SetTerminationProtection	Grants permission to add and remove termination protection for a cluster	Write	cluster*		
SetUnhealthyNodeReplacement	Grants permission to enable or disable unhealthy node replacement for a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetVisibleToAllUsers	Grants permission to set whether all AWS Identity and Access Management (IAM) users in the AWS account can view a cluster. This API is deprecated and your cluster may be visible to all users in your account. To restrict cluster access using an IAM policy, see AWS Identity and Access Management for Amazon EMR (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-access-iam.html)	Write	cluster*		
StartEditor [permission only]	Grants permission to start an EMR notebook	Write	editor* cluster		
StartNotebookExecution	Grants permission to start an EMR notebook execution	Write	cluster* editor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [permission only]	Grants permission to shut down an EMR notebook	Write	editor*		
StopNotebookExecution	Grants permission to stop notebook execution	Write	notebook-execution*		
TerminateJobFlows	Grants permission to terminate a cluster (job flow)	Write	cluster*		
UnlinkRepository [permission only]	Grants permission to unlink an EMR notebook repository from EMR notebooks	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEditor [permission only]	Grants permission to update an EMR notebook	Write	editor*		
UpdateRepository [permission only]	Grants permission to update an EMR notebook repository	Write			
UpdateStudio	Grants permission to update information about an EMR Studio	Write	studio*		
UpdateStudioSessionMapping	Grants permission to update an EMR Studio session mapping	Write	studio*		
ViewEventsFromAllClustersInConsole [permission only]	Grants permission to use the EMR console to view events from all clusters	List			

Resource types defined by Amazon Elastic MapReduce

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
editor	arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
notebook-execution	arn:${Partition}:elasticmapreduce:${Region}:${Account}:notebook-execution/${NotebookExecutionId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
studio	arn:${Partition}:elasticmapreduce:${Region}:${Account}:studio/${StudioId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}

Condition keys for Amazon Elastic MapReduce

Amazon Elastic MapReduce defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by whether the tag and value pair is provided with the action	String
aws:ResourceTag/${TagKey}	Filters access by the tag and value pair associated with an Amazon EMR resource	String
aws:TagKeys	Filters access by whether the tag keys are provided with the action regardless of tag value	ArrayOfString
elasticmapreduce:ExecutionRoleArn	Filters access by whether the execution role ARN is provided with the action	ARN
elasticmapreduce:RequestTag/${TagKey}	Filters access by whether the tag and value pair is provided with the action	String
elasticmapreduce:ResourceTag/${TagKey}	Filters access by the tag and value pair associated with an Amazon EMR resource	String

Actions, resources, and condition keys for Amazon Elastic Transcoder

Amazon Elastic Transcoder (service prefix: `elastictranscoder`) 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 Transcoder

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelJob	Cancel a job that Elastic Transcoder has not begun to process	Write	job*		
CreateJob	Create a job	Write	pipeline*		
			preset*		
CreatePipeline	Create a pipeline	Write			
CreatePreset	Create a preset	Write			
DeletePipeline	Delete a pipeline	Write	pipeline*		
DeletePreset	Delete a preset	Write	preset*		
ListJobsByPipeline	Get a list of the jobs that you assigned to a pipeline	List	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListJobsByStatus	Get information about all of the jobs associated with the current AWS account that have a specified status	List			
ListPipelines	Get a list of the pipelines associated with the current AWS account	List			
ListPresets	Get a list of all presets associated with the current AWS account	List			
ReadJob	Get detailed information about a job	Read	job*		
ReadPipeline	Get detailed information about a pipeline	Read	pipeline*		
ReadPreset	Get detailed information about a preset	Read	preset*		
TestRole	Test the settings for a pipeline to ensure that Elastic Transcoder can create and process jobs	Write			
UpdatePipeline	Update settings for a pipeline	Write	pipeline*		
UpdatePipelineNotifications	Update only Amazon Simple Notification Service (Amazon SNS) notifications for a pipeline	Write	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePipelineStatus	Pause or reactivate a pipeline, so the pipeline stops or restarts processing jobs, update the status for the pipeline	Write	pipeline*		

Resource types defined by Amazon Elastic Transcoder

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:${Partition}:elastictranscoder:${Region}:${Account}:job/${JobId}`	
pipeline	`arn:${Partition}:elastictranscoder:${Region}:${Account}:pipeline/${PipelineId}`	
preset	`arn:${Partition}:elastictranscoder:${Region}:${Account}:preset/${PresetId}`	

Condition keys for Amazon Elastic Transcoder

Elastic Transcoder has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Elastic VMware Service

Amazon Elastic VMware Service (service prefix: `evs`) 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 VMware Service
- Resource types defined by Amazon Elastic VMware Service
- Condition keys for Amazon Elastic VMware Service

Actions defined by Amazon Elastic VMware Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateEipToVlan	Grants permission to associate an Elastic IP address (EIP) with a public VLAN in an Amazon EVS environment	Write	environment*		ec2:AssociateAddress ec2:DescribeAddresses
CreateEnvironment	Grants permission to create an Amazon EVS environment	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateSubnet ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteSubnet ec2:DeleteVolume ec2:DescribeAddresses

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeDhcpOptions ec2:DescribeHosts ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeKeyPairs ec2:DescribeNetworkInterfaces ec2:DescribePlacementGroups ec2:DescribeRouteServerEndpoints

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeRouteServerPeers ec2:DescribeRouteServers ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVolumes ec2:DescribeVpcs ec2:DetachNetworkInterface ec2:DetachVolume ec2:GetAllowedImag

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					esSettings ec2:GetRouteServerAssociations ec2:ModifyInstanceAttribute ec2:ModifyNetworkInterfaceAttribute ec2:RunInstances ec2:TerminateInstances iam:CreateServiceLinkedRole kms:DescribeKey kms:ListAliases

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:GetRandomPassword secretsmanager:GetSecretValue secretsmanager:TagResource secretsmanager:UpdateSecret servicequotas:GetServiceQuota servicequotas:List

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ServiceQuotas support:DescribeServices support:DescribeSupportLevel

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironmentHost	Grants permission to add host to an Amazon EVS environment	Write	environment*		ec2:CreateNetworkInterface ec2:CreateTags ec2:DeleteNetworkInterface ec2:DescribeDhcpOptions ec2:DescribeHosts ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeKeyPairs ec2:DescribeNetworkInterfaces

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribePlacementGroups ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute ec2:RunInstances evs:CreateEnvironmentHost secretsmanager:CreateSecret secretsmanager:DeleteSecret

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:GetRandomPassword secretsmanager:GetSecretValue secretsmanager:TagResource secretsmanager:UpdateSecret servicequotas:GetServiceQuota servicequotas:ListServiceQuotas

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEnvironment	Grants permission to delete an Amazon EVS environment	Write	environment*		ec2:DeleteNetworkInterface ec2:DeleteSubnet ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyInstanceAttribute ec2:ModifyNetworkInterfaceAttribute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:TerminateInstances secretsmanager:DeleteSecret secretsmanager:GetSecretValue

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEnvironmentHost	Grants permission to delete a host from an Amazon EVS environment	Write	environment*		ec2:DeleteNetworkInterface ec2:DescribeInstanceStatus ec2:DescribeInstances ec2:DescribeNetworkInterfaces ec2:ModifyInstanceAttribute ec2:ModifyNetworkInterfaceAttribute ec2:TerminateInstances secretsmanager:DeleteSecret

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:GetSecretValue
DisassociateEipFromVlan	Grants permission to disassociate an Elastic IP address (EIP) from a public VLAN in an Amazon EVS environment	Write	environment*		ec2:DisassociateAddress
GetEnvironment	Grants permission to get an Amazon EVS environment	Read	environment*		
GetVersions	Grants permission to get versions provided for launch by Amazon EVS	Read			
ListEnvironmentHosts	Grants permission to retrieve a list of hosts associated with an Amazon EVS environment	List	environment*		
ListEnvironmentVlans	Grants permission to retrieve a list of Amazon EVS environment VLANs	List	environment*		
ListEnvironments	Grants permission to retrieve a list of Amazon EVS environments in an account	List			
ListTagsForResource	Grants permission to list the tags on a specified resource ARN	Read	environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a specified resource ARN	Tagging	environment*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a specified resource ARN	Tagging	environment*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Resource types defined by Amazon Elastic VMware 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
environment	`arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentIdentifier}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Elastic VMware Service

Amazon Elastic VMware Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${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 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

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		
			parameter group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyServerlessCacheSnapshot	Grants permission to make a copy of an existing serverless cache snapshot	Write	serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshot	Grants permission to make a copy of an existing snapshot	Write	snapshot*		elasticache:AddTagsToResource 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 elasticache:KmsKeyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCacheCluster	Grants permission to create a cache cluster	Write	parametergroup*		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/${TagKey}	
CreateCacheParameterGroup	Grants permission to create a parameter group	Write	parametergroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${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	parameter group*		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	serverlesscache*	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
			serverlesscachesnapshot	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	parameter group*		
				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
			serverlescachesnapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteServerlessCacheSnapshot	Grants permission to delete a serverless cache snapshot	Write	serverlesscachesnapshot*	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/${TagKey}	
DescribeReservedCacheNodesOfferings	Grants permission to list available reserved cache node offerings	List			
DescribeServerlessCacheSnapshots	Grants permission to list information about serverless cache snapshots	List	serverlesscachesnapshot*	aws:ResourceTag/${TagKey}	
			serverlesscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	Grants permission to list serverless caches	List	serverlesscache*	aws:ResourceTag/${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	serverlesscachesnapshot*	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
			serverlesscachesnapshot		
			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	
			parameter group		
			securitygroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	Grants permission to modify parameters of a cache parameter group	Write	parameter group*		
				aws:ResourceTag/${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		
			parametergroup		
			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.

Note

The resource name in the ARN string should be lowercase to be effective.

Resource types	ARN	Condition keys
parameter group	`arn:${Partition}:elasticache:${Region}:${Account}:parametergroup:${CacheParameterGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName

Resource types	ARN	Condition keys
securitygroup	arn:${Partition}:elasticache:${Region}:${Account}:securitygroup:${CacheSecurityGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} 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 AWS 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 AWS Elemental Appliances and Software

AWS Elemental Appliances and Software (service prefix: `elemental-appliances-software`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elemental Appliances and Software

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteUpload [permission only]	Grants permission to complete an upload of an attachment for a quote or order	Write			
CreateOrderV1 [permission only]	Grants permission to create an order	Write			
CreateQuote [permission only]	Grants permission to create a quote	Write	quote*		
GetAvsCorrectAddress [permission only]	Grants permission to validate an address	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBillingAddresses [permission only]	Grants permission to list the billing addresses in the AWS Account	Read			
GetDeliveryAddressesV2 [permission only]	Grants permission to list the delivery addresses in the AWS Account	Read			
GetOrder [permission only]	Grants permission to describe an order	Read			
GetOrdersV2 [permission only]	Grants permission to list the orders in the AWS Account	Read			
GetQuote [permission only]	Grants permission to describe a quote	Read	quote*		
GetTaxes [permission only]	Grants permission to calculate taxes for an order	Read			
ListQuotes [permission only]	Grants permission to list the quotes in the AWS Account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartUpload [permission only]	Grants permission to start an upload of an attachment for a quote or order	Write			
SubmitOrderV1 [permission only]	Grants permission to submit an order	Write			
UpdateQuote [permission only]	Grants permission to modify a quote	Write	quote*		

Resource types defined by AWS Elemental Appliances and Software

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
quote	`arn:${Partition}:elemental-appliances-software:${Region}:${Account}:quote/${ResourceId}`	

Condition keys for AWS Elemental Appliances and Software

Elemental Appliances and Software has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Elemental Appliances and Software Activation Service

AWS Elemental Appliances and Software Activation Service (service prefix: `elemental-activations`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elemental Appliances and Software Activation Service
- Resource types defined by AWS Elemental Appliances and Software Activation Service
- Condition keys for AWS Elemental Appliances and Software Activation Service

Actions defined by AWS Elemental Appliances and Software Activation Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteAccountReg	Grants permission to complete the process of	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
istration [permission only]	registering customer account for AWS Elemental Appliances and Software Purchases				
CompleteFileUpload [permission only]	Grants permission to complete the process of uploading a Software file for AWS Elemental Appliances and Software Purchases	Write			
ConfirmAccount [permission only]	Grants permission to confirm asset ownership	Write			
DownloadKickstart [permission only]	Grants permission to download the kickstart files for AWS Elemental Appliances and Software purchases	Read			
DownloadSoftware [permission only]	Grants permission to download the Software files for AWS Elemental Appliances and Software Purchases	Read			
GenerateLicense [permission only]	Grants permission to generate a software license for an AWS Elemental Appliances and Software purchase	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateLicenses [permission only]	Grants permission to generate Software Licenses for AWS Elemental Appliances and Software Purchases	Write			
GetArtifactGroupSoftwareVersions [permission only]	Grants permission to describe the software version of an artifact group	Read			
GetAsset [permission only]	Grants permission to describe an asset	Read			
GetAssets [permission only]	Grants permission to describe assets associated to the requesting account	Read			
GetProductAdvisories [permission only]	Grants permission to get all product advisories	Read			
GetSoftwareVersions [permission only]	Grants permission to describe available software versions	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartFileUpload [permission only]	Grants permission to start the process of uploading a Software file for AWS Elemental Appliances and Software Purchases	Write			

Resource types defined by AWS Elemental Appliances and Software Activation Service

AWS Elemental Appliances and Software Activation Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Elemental Appliances and Software Activation Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Elemental Appliances and Software Activation Service

Elemental Activations has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Elemental Inference

AWS Elemental Inference (service prefix: `elemental-inference`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elemental Inference
- Resource types defined by AWS Elemental Inference
- Condition keys for AWS Elemental Inference

Actions defined by AWS Elemental Inference

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFeed	Grants permission to associate a feed with an AWS resource	Write	feed*		
CreateFeed	Grants permission to create a new feed	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFeed	Grants permission to delete a feed	Write	feed*		
DisassociateFeed	Grants permission to disassociate a feed from an AWS resource	Write	feed*		
GetFeed	Grants permission to get feed details	Read	feed*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMetadata	Grants permission to retrieve metadata for a specific feed output	Read	feed*		
ListFeeds	Grants permission to list feeds in the account	List			
ListTagsForResource	Grants permission to list tags on a resource	Read			
PutMedia	Grants permission to upload media data for a specified feed	Write	feed*		
TagResource	Grants permission to add tags to a resource	Tagging	feed		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	feed		
				aws:TagKeys	
UpdateFeed	Grants permission to update feed configuration	Write	feed*		

Resource types defined by AWS Elemental Inference

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
feed	`arn:${Partition}:elemental-inference:${Region}:${Account}:feed/${Id}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental Inference

AWS Elemental Inference defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental MediaConnect

AWS Elemental MediaConnect (service prefix: `mediaconnect`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elemental MediaConnect

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddBridgeOutputs	Grants permission to add outputs to an existing bridge	Write	Bridge*		
AddBridgeSources	Grants permission to add sources to an existing bridge	Write	Bridge*		
AddFlowMediaStreams	Grants permission to add media streams to any flow	Write	Flow*		
			MediaStream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
AddFlowOutputs	Grants permission to add outputs to any flow	Write	Flow*		
			Output*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddFlowSources	Grants permission to add sources to any flow	Write	Flow*		
			Source*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddFlowVpcInterfaces	Grants permission to add VPC interfaces to any flow	Write	Flow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VpcInterface*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateRouterNetworkInterface	Grants permission to associate a router network interface	Write			
CreateBridge	Grants permission to create bridges	Write	Bridge*		
CreateFlow	Grants permission to create flows	Write	Flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	Grants permission to create gateways	Write	Gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouterInput	Grants permission to create a new router input in AWS Elemental MediaConnect	Write	RouterInput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:CreateRouterInput mediaconnect:TagResource mediaconnect:UpdateFlowOutput

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouterNetworkInterface	Grants permission to create a new router network interface in AWS Elemental MediaConnect	Write	RouterNetworkInterface*		iam:CreateServiceLinkedRole mediaconnect:CreateRouterNetworkInterface mediaconnect:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouterOutput	Grants permission to create a new router output in AWS Elemental MediaConnect	Write	RouterOutput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:CreateRouterOutput mediaconnect:TagResource mediaconnect:UpdateFlowSource medialive:UpdateInput

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBridge	Grants permission to delete bridges	Write	Bridge*		
DeleteFlow	Grants permission to delete flows	Write	Flow*		
DeleteGateway	Grants permission to delete gateways	Write	Gateway*		
DeleteRouterInput	Grants permission to delete a router input in AWS Elemental MediaConnect	Write	RouterInput*		
DeleteRouterNetworkInterface	Grants permission to delete a router network interface from AWS Elemental MediaConnect	Write	RouterNetworkInterface*		
DeleteRouterOutput	Grants permission to delete a router output from AWS Elemental MediaConnect	Write	RouterOutput*		
DeregisterGatewayInstance	Grants permission to deregister gateway instance	Write	GatewayInstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBridge	Grants permission to display the details of a bridge	Read	Bridge*		
DescribeFlow	Grants permission to display the details of a flow including the flow ARN, name, and Availability Zone, as well as details about the source, outputs, and entitlements	Read	Flow*		
DescribeFlowSourceMetadata	Grants permission to view information about the flow's source transport stream and programs	Read	Flow*		
DescribeFlowSourceThumbnail	Grants permission to view flow's source thumbnail	Read	Flow*		
DescribeGateway	Grants permission to display the details of a gateway including the gateway ARN, name, and CIDR blocks, as well as details about the networks	Read	Gateway*		
DescribeGatewayInstance	Grants permission to display the details of a gateway instance	Read	GatewayInstance*		
DescribeOffering	Grants permission to display the details of an offering	Read	Offering*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservation	Grants permission to display the details of a reservation	Read	Reservation*		
DiscoverGatewayPollEndpoint	Grants permission to discover gateway poll endpoint	Read	Gateway*		
GetRouterInput	Grants permission to retrieve information about a specific router input in AWS Elemental MediaConnect	Read	RouterInput*		
GetRouterInputSourceMetadata	Grants permission to retrieve metadata about a router input source in AWS Elemental MediaConnect	Read	RouterInput*		
GetRouterInputThumbnail	Grants permission to retrieve the thumbnail for a router input in AWS Elemental MediaConnect	Read	RouterInput*		
GetRouterNetworkInterface	Grants permission to retrieve information about a specific router network interface in AWS Elemental MediaConnect	Read	RouterNetworkInterface*		
GetRouterOutput	Grants permission to retrieve information about a specific router output in AWS Elemental MediaConnect	Read	RouterOutput*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GrantFlowEntitlements	Grants permission to grant entitlements on any flow	Write	Entitlement*		
			Flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListBridges	Grants permission to display a list of bridges that are associated with this account and an optionally specified Arn	List			
ListEntitlements	Grants permission to display a list of all entitlements that have been granted to the account	List			
ListFlows	Grants permission to display a list of flows that are associated with this account	List			
ListGatewayInstances	Grants permission to display a list of instances that are associated with this gateway	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGateways	Grants permission to display a list of gateways that are associated with this account	List			
ListOfferings	Grants permission to display a list of all offerings that are available to the account in the current AWS Region	List			
ListReservations	Grants permission to display a list of all reservations that have been purchased by the account in the current AWS Region	List			
ListRouterInputs	Grants permission to retrieve a list of router inputs in AWS Elemental MediaConnect	List			
ListRouterNetworkInterfaces	Grants permission to retrieve a list of router network interfaces in AWS Elemental MediaConnect	List			
ListRouterOutputs	Grants permission to retrieve a list of router outputs in AWS Elemental MediaConnect	List			
ListTagsForResource	Grants permission to display a list of all tags associated with a resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PollGateway	Grants permission to poll gateway	Write			
PurchaseOffering	Grants permission to purchase an offering	Write	Reservation*		
RemoveBridgeOutput	Grants permission to remove an output of an existing bridge	Write	Bridge*		
RemoveBridgeSource	Grants permission to remove a source of an existing bridge	Write	Bridge*		
RemoveFlowMediaStream	Grants permission to remove media streams from any flow	Write	Flow*		
			MediaStream*		
RemoveFlowOutput	Grants permission to remove outputs from any flow	Write	Flow*		
			Output*		
RemoveFlowSource	Grants permission to remove sources from any flow	Write	Flow*		
			Source*		
RemoveFlowVpcInterface	Grants permission to remove VPC interfaces from any flow	Write	Flow*		
			VpcInterface*		
RestartRouterInput	Grants permission to restart a router input in AWS Elemental MediaConnect	Write	RouterInput*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestartRouterOutput	Grants permission to restart a router output in AWS Elemental MediaConnect	Write	RouterOutput*		
RevokeFlowEntitlement	Grants permission to revoke entitlements on any flow	Write	Entitlement*		
			Flow*		
StartFlow	Grants permission to start flows	Write	Flow*		
StartRouterInput	Grants permission to start a router input in AWS Elemental MediaConnect	Write	RouterInput*		
StartRouterOutput	Grants permission to start a router output in AWS Elemental MediaConnect	Write	RouterOutput*		
StopFlow	Grants permission to stop flows	Write	Flow*		
StopRouterInput	Grants permission to stop a router input in AWS Elemental MediaConnect	Write	RouterInput*		
StopRouterOutput	Grants permission to stops a router output in AWS Elemental MediaConnect	Write	RouterOutput*		
SubmitGatewayStateChange	Grants permission to submit gateway state change	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to associate tags with resources	Tagging	Entitlement		
			Flow		
			MediaStream		
			Output		
			RouterInput		
			RouterNetworkInterface		
			RouterOutput		
			Source		
			VpcInterface		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TakeRouterInput	Grants permission to associate a router input with a router output in AWS Elemental MediaConnect	Write	RouterOutput*		
UntagResource	Grants permission to remove tags from resources	Tagging	Entitlement		
			Flow		
			MediaStream		
			Output		
			RouterInput		
			RouterNetworkInterface		
			RouterOutput		
			Source		
			VpcInterface		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBridge	Grants permission to update bridges	Write	Bridge*		
UpdateBridgeOutput	Grants permission to update an output of an existing bridge	Write	Bridge*		
UpdateBridgeSource	Grants permission to update a source of an existing bridge	Write	Bridge*		
UpdateBridgeState	Grants permission to update the state of an existing bridge	Write	Bridge*		
UpdateFlow	Grants permission to update flows	Write	Flow*		
UpdateFlowEntitlement	Grants permission to update entitlements on any flow	Write	Flow*		
UpdateFlowMediaStream	Grants permission to update media streams on any flow	Write	Flow*		
			MediaStream*		
UpdateFlowOutput	Grants permission to update outputs on any flow	Write	Flow*		
			Output*		
UpdateFlowSource	Grants permission to update the source of any flow	Write	Flow*		
			Source*		
UpdateGatewayInstance	Grants permission to update the configuration of an existing Gateway Instance	Write	GatewayInstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRouterInput	Grants permission to update the configuration of a router input in AWS Elemental MediaConnect	Write	RouterInput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:UpdateFlowOutput mediaconnect:UpdateRouterInput
UpdateRouterNetworkInterface	Grants permission to updated the configuration of a router network interface in AWS Elemental MediaConnect	Write	RouterNetworkInterface*		iam:CreateServiceLinkedRole mediaconnect:UpdateRouterNetworkInterface

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRouterOutput	Grants permission to update the configuration of a router output in AWS Elemental MediaConnect	Write	RouterOutput*		ec2:CreateNetworkInterface iam:PassRole mediaconnect:AssociateRouterNetworkInterface mediaconnect:UpdateFlowSource mediaconnect:UpdateRouterOutput medialive:UpdateInput

Resource types defined by AWS Elemental MediaConnect

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
Bridge	arn:${Partition}:mediaconnect:${Region}:${Account}:bridge:${BridgeId}:${BridgeName}	
Entitlement	arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${FlowId}:${EntitlementName}	aws:ResourceTag/${TagKey}
Flow	arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}	aws:ResourceTag/${TagKey}
Gateway	arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}	
GatewayInstance	arn:${Partition}:mediaconnect:${Region}:${Account}:gateway:${GatewayId}:${GatewayName}:instance:${InstanceId}	
MediaStream	arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}/mediaStream/${MediaStreamName}	aws:ResourceTag/${TagKey}
Offering	arn:${Partition}:mediaconnect:${Region}:offering:${OfferingId}	
Output	arn:${Partition}:mediaconnect:${Region}:${Account}:output:${OutputId}:${OutputName}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Reservation	arn:${Partition}:mediaconnect:${Region}:${Account}:reservation:${ReservationId}:${ReservationName}	
RouterInput	arn:${Partition}:mediaconnect:${Region}:${Account}:routerInput:${RouterInputId}	aws:ResourceTag/${TagKey}
RouterNetworkInterface	arn:${Partition}:mediaconnect:${Region}:${Account}:routerNetworkInterface:${RouterNetworkInterfaceId}	aws:ResourceTag/${TagKey}
RouterOutput	arn:${Partition}:mediaconnect:${Region}:${Account}:routerOutput:${RouterOutputId}	aws:ResourceTag/${TagKey}
Source	arn:${Partition}:mediaconnect:${Region}:${Account}:source:${SourceId}:${SourceName}	aws:ResourceTag/${TagKey}
VpcInterface	arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${FlowId}:${FlowName}/vpcInterface/${VpcInterfaceName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental MediaConnect

AWS Elemental MediaConnect defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental MediaConvert

AWS 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 AWS Elemental MediaConvert
- Resource types defined by AWS Elemental MediaConvert
- Condition keys for AWS Elemental MediaConvert

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Certificate	Grants permission to associate an AWS Certificate Manager (ACM) Amazon Resource Name (ARN) with AWS Elemental MediaConvert	Write			
CancelJob	Grants permission to cancel an AWS Elemental MediaConvert job that is waiting in queue	Write	Job*		
CreateJob	Grants permission to create and submit an AWS Elemental MediaConvert job	Write	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys mediaconvert:HttpInputsAllowed mediaconvert:Https	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				InputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Grants permission to create an AWS Elemental MediaConvert custom job template	Write	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePreset	Grants permission to create an AWS Elemental MediaConvert custom output preset	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQueue	Grants permission to create an AWS Elemental MediaConvert job queue	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateResourceShare	Grants permission to share an AWS Elemental MediaConvert job	Write	Job		
DeleteJobTemplate	Grants permission to delete an AWS Elemental MediaConvert custom job template	Write	JobTemplate*		
DeletePolicy	Grants permission to delete an AWS Elemental MediaConvert policy	Write			
DeletePreset	Grants permission to delete an AWS Elemental MediaConvert custom output preset	Write	Preset*		
DeleteQueue	Grants permission to delete an AWS Elemental MediaConvert job queue	Write	Queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEndpoints	Grants permission to subscribe to the AWS 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 AWS Certificate Manager (ACM) certificate and an AWS Elemental MediaConvert resource	Write			
GetJob	Grants permission to get an AWS Elemental MediaConvert job	Read	Job*		
GetJobTemplate	Grants permission to get an AWS Elemental MediaConvert job template	Read	JobTemplate*		
GetPolicy	Grants permission to get an AWS Elemental MediaConvert policy	Read			
GetPreset	Grants permission to get an AWS Elemental MediaConvert output preset	Read	Preset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQueue	Grants permission to get an AWS Elemental MediaConvert job queue	Read	Queue*		
ListJobTemplates	Grants permission to list AWS Elemental MediaConvert job templates	List			
ListJobs	Grants permission to list AWS Elemental MediaConvert jobs	List	Queue		
ListPresets	Grants permission to list AWS Elemental MediaConvert output presets	List			
ListQueues	Grants permission to list AWS 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 AWS Elemental MediaConvert job engine versions	List			
Probe	Grants permission to probe a file	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPolicy	Grants permission to put an AWS Elemental MediaConvert policy	Write			
SearchJobs	Grants permission to search AWS Elemental MediaConvert jobs	List	Queue		
TagResource	Grants permission to add tags to a MediaConvert queue, preset, or job template	Tagging	Job		
			JobTemplate		
			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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateJobTemplate	Grants permission to update an AWS Elemental MediaConvert custom job template	Write	JobTemplate*		
			Preset		
			Queue		
UpdatePreset	Grants permission to update an AWS Elemental MediaConvert custom output preset	Write	Preset*		
UpdateQueue	Grants permission to update an AWS Elemental MediaConvert job queue	Write	Queue*		

Resource types defined by AWS 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}

Resource types	ARN	Condition keys
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 AWS Elemental MediaConvert

AWS 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 AWS 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

Condition keys	Description	Type
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 AWS Elemental MediaLive

AWS Elemental MediaLive (service prefix: `medialive`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elemental MediaLive
- Resource types defined by AWS Elemental MediaLive
- Condition keys for AWS Elemental MediaLive

Actions defined by AWS Elemental MediaLive

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptInputDeviceTransfer	Grants permission to accept an input device transfer	Write	input-device*		
BatchDelete	Grants permission to delete channels, inputs, input security groups, and multiplexes	Write			
BatchStart	Grants permission to start channels and multiplexes	Write			
BatchStop	Grants permission to stop channels and multiplexes	Write			
BatchUpdateSchedule	Grants permission to add and remove actions from a channel's schedule	Write	channel*		
CancelInputDeviceTransfer	Grants permission to cancel an input device transfer	Write	input-device*		
ClaimDevice	Grants permission to claim an input device	Write	input-device*		
CreateChannel	Grants permission to create a channel	Write	channel*		
			input*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateChannelPlacementGroup	Grants permission to create a cluster	Write	channel-placement-group*		
			cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplate	Grants permission to create a cloudwatch alarm template	Write	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudWatchAlarmTemplateGroup	Grants permission to create a cloudwatch alarm template group	Write	cloudwatch-alarm-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCluster	Grants permission to create a cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventBridgeRuleTemplate	Grants permission to create a eventbridge rule template	Write	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventBridgeRuleTemplateGroup	Grants permission to create a eventbridge rule template group	Write	eventbridge-rule-template-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Grants permission to create an input	Write	input*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInputSecurityGroup	Grants permission to create an input security group	Write	input-security-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiplex	Grants permission to create a multiplex	Write	multiplex*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMultiplexProgram	Grants permission to create a multiplex program	Write	multiplex*		
CreateNetwork	Grants permission to create a network	Write	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNode	Grants permission to create a node	Write	cluster*		
			node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodeRegistrationScript	Grants permission to create a node registration script	Write	cluster*		
CreatePartnerInput	Grants permission to create a partner input	Write	input*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSdiSource	Grants permission to create a SDI source	Write	sdi-source*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalMap	Grants permission to create a signal map	Write	signal-map*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTags	Grants permission to create tags for channels, inputs, input security groups, multiplexes, reservations, nodes, networks, clusters, channel placement groups, signal maps, SDI sources, template groups, and templates	Tagging	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Grants permission to delete a channel	Write	channel*		
DeleteChannelPlacementGroup	Grants permission to delete a cluster	Write	channel-placement-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCloudWatchAlarmTemplate	Grants permission to delete a cloudwatch alarm template	Write	cloudwatch-alarm-template*		
DeleteCloudWatchAlarmTemplateGroup	Grants permission to delete a cloudwatch alarm template group	Write	cloudwatch-alarm-template-group*		
DeleteCluster	Grants permission to delete a cluster	Write	cluster*		
DeleteEventBridgeRuleTemplate	Grants permission to delete a eventbridge rule template	Write	eventbridge-rule-template*		
DeleteEventBridgeRuleTemplateGroup	Grants permission to delete a eventbridge rule template group	Write	eventbridge-rule-template-group*		
DeleteInput	Grants permission to delete an input	Write	input*		
DeleteInputSecurityGroup	Grants permission to delete an input security group	Write	input-security-group*		
DeleteMultiplex	Grants permission to delete a multiplex	Write	multiplex*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMultiplexProgram	Grants permission to delete a multiplex program	Write	multiplex*		
DeleteNetwork	Grants permission to delete a network	Write	network*		
DeleteNode	Grants permission to delete a node	Write	node*		
DeleteReservation	Grants permission to delete an expired reservation	Write	reservation*		
DeleteSchedule	Grants permission to delete all schedule actions for a channel	Write	channel*		
DeleteSdiSource	Grants permission to delete a SDI source	Write	sdi-source*		
DeleteSignalMap	Grants permission to delete a signal map	Write	signal-map*		
DeleteTags	Grants permission to delete tags from channels, inputs, input security groups, multiplexes, reservations, nodes, clusters, networks, channel placement groups, SDI source, signal maps, template groups, and templates	Tagging	channel		
			channel-placement-group		
			cloudwatch-alarm-template		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		
			multiplex		
			network		
			node		
			reservation		
			sdi-source		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			signal-map		
				aws:TagKeys	
DescribeAccountConfiguration	Grants permission to view the account configuration of the customer	Read			
DescribeChannel	Grants permission to get details about a channel	Read	channel*		
DescribeChannelPlacementGroup	Grants permission to describe a channel placement group	Read	channel-placement-group*		
DescribeCluster	Grants permission to describe a cluster	Read	cluster*		
DescribeInput	Grants permission to describe an input	Read	input*		
DescribeInputDevice	Grants permission to describe an input device	Read	input-device*		
DescribeInputDeviceThumbnail	Grants permission to describe an input device thumbnail	Read	input-device*		
DescribeInputSecurityGroup	Grants permission to describe an input security group	Read	input-security-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMultiplex	Grants permission to describe a multiplex	Read	multiplex*		
DescribeMultiplexProgram	Grants permission to describe a multiplex program	Read	multiplex*		
DescribeNetwork	Grants permission to describe a network	Read	network*		
DescribeNode	Grants permission to describe a node	Read	node*		
DescribeOffering	Grants permission to get details about a reservation offering	Read	offering*		
DescribeReservation	Grants permission to get details about a reservation	Read	reservation*		
DescribeSchedule	Grants permission to view a list of actions scheduled on a channel	Read	channel*		
DescribeSdiSource	Grants permission to describe a SDI source	Read	sdi-source*		
DescribeThumbnails	Grants permission to view the thumbnails for a channel	Read	channel*		
GetCloudWatchAlarmTemplate	Grants permission to get a cloudwatch alarm template	Read	cloudwatch-alarm-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCloudWatchAlarmTemplateGroup	Grants permission to get a cloudwatch alarm template group	Read	cloudwatch-alarm-template-group*		
GetEventBridgeRuleTemplate	Grants permission to get a eventbridge rule template	Read	eventbridge-rule-template*		
GetEventBridgeRuleTemplateGroup	Grants permission to get a eventbridge rule template group	Read	eventbridge-rule-template-group*		
GetSignalMap	Grants permission to get a signal map	Read	signal-map*		
ListAlerts	Grants permission to list channel alerts	List			
ListChannelPlacementGroups	Grants permission to list channel placement groups	List			
ListChannels	Grants permission to list channels	List			
ListCloudWatchAlarmTemplateGroups	Grants permission to list cloudwatch alarm template groups	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCloudWatchAlarmTemplates	Grants permission to list cloudwatch alarm templates	List			
ListClusterAlerts	Grants permission to list cluster alerts	List			
ListClusters	Grants permission to list clusters	List			
ListEventBridgeRuleTemplateGroups	Grants permission to list eventbridge rule template groups	List			
ListEventBridgeRuleTemplates	Grants permission to list eventbridge rule templates	List			
ListInputDeviceTransfers	Grants permission to list input device transfers	List			
ListInputDevices	Grants permission to list input devices	List			
ListInputSecurityGroups	Grants permission to list input security groups	List			
ListInputs	Grants permission to list inputs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMultiplexAlerts	Grants permission to list multiplex alerts	List			
ListMultiplexPrograms	Grants permission to list multiplex programs	List			
ListMultiplexes	Grants permission to list multiplexes	List			
ListNetworks	Grants permission to list networks	List			
ListNodes	Grants permission to list nodes	List			
ListOfferings	Grants permission to list reservation offerings	List			
ListReservations	Grants permission to list reservations	List			
ListSdiSources	Grants permission to list SDI sources	List			
ListSignalMaps	Grants permission to list signal maps	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for channels, inputs, input security groups, multiplexes, reservations, nodes, clusters, networks, channel placement groups, SDI sources, signal maps, template groups, and templates	List	channel		
			channel-placement-group		
			cloudwatch-alarm-template		
			cloudwatch-alarm-template-group		
			cluster		
			eventbridge-rule-template		
			eventbridge-rule-template-group		
			input		
			input-security-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			multiplex		
			network		
			node		
			reservation		
			sdi-source		
			signal-map		
ListVersions	Grants permission to list available versions of MediaLive	List			
PollAnywhere	Grants permission to the node to poll the cluster	Write			
PurchaseOffering	Grants permission to purchase a reservation offering	Write	offering*		
			reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RebootInputDevice	Grants permission to reboot an input device	Write	input-device*		
RejectInputDeviceTransfer	Grants permission to reject an input device transfer	Write	input-device*		
RestartChannelPipelines	Grants permission to restart pipelines on a running channel	Write	channel*		
StartChannel	Grants permission to start a channel	Write	channel*		
StartDeleteMonitorDeployment	Grants permission to start deletion of a signal map's monitor	Write	signal-map*		
StartInputDevice	Grants permission to start an input device attached to a MediaConnect flow	Write	input-device*		
StartInputDeviceMaintenanceWindow	Grants permission to start a maintenance window for an input device	Write	input-device*		
StartMonitorDeployment	Grants permission to start a signal map monitor deployment	Write	signal-map*		
StartMultiplex	Grants permission to start a multiplex	Write	multiplex*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartUpdateSignalMap	Grants permission to start a signal map update	Write	signal-map*		
StopChannel	Grants permission to stop a channel	Write	channel*		
StopInputDevice	Grants permission to stop an input device attached to a MediaConnect flow	Write	input-device*		
StopMultiplex	Grants permission to stop a multiplex	Write	multiplex*		
SubmitAnywhereStateChange	Grants permission to the node to submit state changes to the cluster	Write			
TransferInputDevice	Grants permission to transfer an input device	Write	input-device*		
UpdateAccountConfiguration	Grants permission to update a customer's account configuration	Write			
UpdateChannel	Grants permission to update a channel	Write	channel*		
UpdateChannelClass	Grants permission to update the class of a channel	Write	channel*		
UpdateChannelPlacementGroup	Grants permission to update a node	Write	channel-placement-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateCloudWatchAlarmTemplate	Grants permission to update a cloudwatch alarm template	Write	cloudwatch-alarm-template*		
			cloudwatch-alarm-template-group*		
UpdateCloudWatchAlarmTemplateGroup	Grants permission to update a cloudwatch alarm template group	Write	cloudwatch-alarm-template-group*		
UpdateCluster	Grants permission to update a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEventBridgeRuleTemplate	Grants permission to update a eventbridge rule template	Write	eventbridge-rule-template*		
			eventbridge-rule-template-group*		
UpdateEventBridgeRuleTemplateGroup	Grants permission to update a eventbridge rule template group	Write	eventbridge-rule-template-group*		
UpdateInput	Grants permission to update an input	Write	input*		
UpdateInputDevice	Grants permission to update an input device	Write	input-device*		
UpdateInputSecurityGroup	Grants permission to update an input security group	Write	input-security-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateMultiplex	Grants permission to update a multiplex	Write	multiplex*		
UpdateMultiplexProgram	Grants permission to update a multiplex program	Write	multiplex*		
UpdateNetwork	Grants permission to update the state of a node	Write	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateNode	Grants permission to update a node	Write	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNodeState	Grants permission to update the state of a node	Write	node*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateReservation	Grants permission to update a reservation	Write	reservation*		
UpdateSdiSource	Grants permission to update the state of a sdi source	Write	sdi-source*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Resource types defined by AWS Elemental MediaLive

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:${Partition}:medialive:${Region}:${Account}:channel:${ChannelId}	aws:ResourceTag/${TagKey}
input	arn:${Partition}:medialive:${Region}:${Account}:input:${InputId}	aws:ResourceTag/${TagKey}
input-device	arn:${Partition}:medialive:${Region}:${Account}:inputDevice:${DeviceId}	
input-security-group	arn:${Partition}:medialive:${Region}:${Account}:inputSecurityGroup:${InputSecurityGroupId}	aws:ResourceTag/${TagKey}
multiplex	arn:${Partition}:medialive:${Region}:${Account}:multiplex:${MultiplexId}	aws:ResourceTag/${TagKey}
reservation	arn:${Partition}:medialive:${Region}:${Account}:reservation:${ReservationId}	aws:ResourceTag/${TagKey}
offering	arn:${Partition}:medialive:${Region}:${Account}:offering:${OfferingId}	
signal-map	arn:${Partition}:medialive:${Region}:${Account}:signal-map:${SignalMapId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template-group	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template-group:${CloudWatchAlarmTemplateGroupId}	aws:ResourceTag/${TagKey}
cloudwatch-alarm-template	arn:${Partition}:medialive:${Region}:${Account}:cloudwatch-alarm-template:${CloudWatchAlarmTemplateId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
eventbridge-rule-template-group	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template-group:${EventBridgeRuleTemplateGroupId}	aws:ResourceTag/${TagKey}
eventbridge-rule-template	arn:${Partition}:medialive:${Region}:${Account}:eventbridge-rule-template:${EventBridgeRuleTemplateId}	aws:ResourceTag/${TagKey}
cluster	arn:${Partition}:medialive:${Region}:${Account}:cluster:${ClusterId}	aws:ResourceTag/${TagKey}
node	arn:${Partition}:medialive:${Region}:${Account}:node:${ClusterId}/${NodeId}	aws:ResourceTag/${TagKey}
network	arn:${Partition}:medialive:${Region}:${Account}:network:${NetworkId}	aws:ResourceTag/${TagKey}
channel-placement-group	arn:${Partition}:medialive:${Region}:${Account}:channelPlacementGroup:${ClusterId}/${ChannelPlacementGroupId}	aws:ResourceTag/${TagKey}
sdi-source	arn:${Partition}:medialive:${Region}:${Account}:sdiSource:${SdiSourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental MediaLive

AWS Elemental MediaLive defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental MediaPackage

AWS Elemental MediaPackage (service prefix: `mediapackage`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elemental MediaPackage
- Resource types defined by AWS Elemental MediaPackage
- Condition keys for AWS Elemental MediaPackage

Actions defined by AWS Elemental MediaPackage

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureLogs	Grants permission to configure access logs for a Channel	Write	channels*		iam:CreateServiceLinkedRole
CreateChannel	Grants permission to create a channel in AWS Elemental MediaPackage	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Grants permission to create a harvest job in AWS Elemental MediaPackage	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOriginEndpoint	Grants permission to create an endpoint in AWS Elemental MediaPackage	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Grants permission to delete a channel in AWS Elemental MediaPackage	Write	channels*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOriginEndpoint	Grants permission to delete an endpoint in AWS Elemental MediaPackage	Write	origin_endpoints*		
DescribeChannel	Grants permission to view the details of a channel in AWS Elemental MediaPackage	Read	channels*		
DescribeHarvestJob	Grants permission to view the details of a harvest job in AWS Elemental MediaPackage	Read	harvest_jobs*		
DescribeOriginEndpoint	Grants permission to view the details of an endpoint in AWS Elemental MediaPackage	Read	origin_endpoints*		
ListChannels	Grants permission to view a list of channels in AWS Elemental MediaPackage	Read			
ListHarvestJobs	Grants permission to view a list of harvest jobs in AWS Elemental MediaPackage	Read			
ListOriginEndpoints	Grants permission to view a list of endpoints in AWS Elemental MediaPackage	Read			
ListTagsForResource	Grants permission to list the tags assigned to a Channel or OriginEndpoint	Read	channels		
			harvest_jobs		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			origin_endpoints		
RotateChannelCredentials	Grants permission to rotate credentials for the first IngestEndpoint of a Channel in AWS Elemental MediaPackage	Write	channels*		
RotateIngestEndpointCredentials	Grants permission to rotate IngestEndpoint credentials for a Channel in AWS Elemental MediaPackage	Write	channels*		
TagResource	Grants permission to tag a MediaPackage resource	Tagging	channels		
			harvest_jobs		
			origin_endpoints		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to delete tags to a Channel or OriginEndpoint	Tagging	channels		
			harvest_jobs		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			origin_endpoints		
				aws:TagKeys	
UpdateChannel	Grants permission to make changes to a channel in AWS Elemental MediaPackage	Write	channels*		
UpdateOriginEndpoint	Grants permission to make changes to an endpoint in AWS Elemental MediaPackage	Write	origin_endpoints*		

Resource types defined by AWS Elemental MediaPackage

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
channels	`arn:${Partition}:mediapackage:${Region}:${Account}:channels/${ChannelIdentifier}`	aws:ResourceTag/${TagKey}
origin_endpoints	`arn:${Partition}:mediapackage:${Region}:${Account}:origin_endpoints/${OriginEndpointIdentifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
harvest_jobs	arn:${Partition}:mediapackage:${Region}:${Account}:harvest_jobs/${HarvestJobIdentifier}	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental MediaPackage

AWS Elemental MediaPackage defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag for a MediaPackage request	String
aws:ResourceTag/${TagKey}	Filters access by the tag for a MediaPackage resource	String
aws:TagKeys	Filters access by the tag keys for a MediaPackage resource or request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental MediaPackage V2

AWS Elemental MediaPackage V2 (service prefix: mediapackagev2) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elemental MediaPackage V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelHarvestJob	Grants permission to cancel a harvest job	Write	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
CreateChannel	Grants permission to create a channel in a channel group	Write	Channel*		
			ChannelGroup*		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateChannelGroup	Grants permission to create a channel group	Write	ChannelGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHarvestJob	Grants permission to create a harvest job	Write	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOriginEndpoint	Grants permission to create an origin endpoint for a channel	Write	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Grants permission to delete a channel in a channel group	Write	Channel*		
			ChannelGroup*		
DeleteChannelGroup	Grants permission to delete a channel group	Write	ChannelGroup*		
DeleteChannelPolicy	Grants permission to delete a resource policy from a channel	Write	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
DeleteOriginEndpoint	Grants permission to delete an origin endpoint of a channel	Write	Channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ChannelGroup*		
			OriginEndpoint*		
DeleteOriginEndpointPolicy	Grants permission to delete a resource policy from an origin endpoint	Write	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
GetChannel	Grants permission to retrieve details of a channel in a channel group	Read	Channel*		
			ChannelGroup*		
GetChannelGroup	Grants permission to retrieve details of a channel group	Read	ChannelGroup*		
GetChannelPolicy	Grants permission to retrieve a resource policy for a channel	Read	Channel*		
			ChannelGroup*		
			ChannelPolicy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHarvestJob	Grants permission to retrieve details of an harvest job	Read	Channel*		
			ChannelGroup*		
			HarvestJob*		
			OriginEndpoint*		
GetHeadObject	Grants permission to make GetHeadObject requests to MediaPackage	Read	OriginEndpoint*		
GetObject	Grants permission to make GetObject requests to MediaPackage	Read	OriginEndpoint*		
GetOriginEndpoint	Grants permission to retrieve details of an origin endpoint	Read	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
GetOriginEndpointPolicy	Grants permission to retrieve details of a resource policy for an origin endpoint	Read	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			OriginEndpointPolicy*		
HarvestObject	Grants permission to make HarvestObject requests to MediaPackage	Read	OriginEndpoint*		
ListChannelGroups	Grants permission to list all channel groups for an aws account	List			
ListChannels	Grants permission to list all channels in a channel group	List	ChannelGroup*		
ListHarvestJobs	Grants permission to list all harvest jobs in a channel group, channel, origin endpoint	List	ChannelGroup*		
ListOriginEndpoints	Grants permission to list all origin endpoints of a channel	List	Channel*		
			ChannelGroup*		
ListTagsForResource	Grants permission to list tags for the specified resource	Read	Channel		
			ChannelGroup		
			HarvestJob		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			OriginEndpoint		
PutChannelPolicy	Grants permission to attach a resource policy for a channel	Write	Channel*		
			ChannelGroup*		
			ChannelPolicy*		
PutObject	Grants permission to make PutObject requests to MediaPackage	Write	Channel*		
PutOriginEndpointPolicy	Grants permission to attach a resource policy to an origin endpoint	Write	Channel*		
			ChannelGroup*		
			OriginEndpoint*		
			OriginEndpointPolicy*		
ResetChannelState	Grants permission to reset a channel	Write	Channel*		
			ChannelGroup*		
ResetOriginEndpointState	Grants permission to reset an origin endpoint	Write	Channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ChannelGroup*		
			OriginEndpoint*		
TagResource	Grants permission to add specified tags to the specified resource	Tagging	Channel		
			ChannelGroup		
			HarvestJob		
			OriginEndpoint		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	Channel		
			ChannelGroup		
			HarvestJob		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			OriginEndpoint		
				aws:TagKeys	
UpdateChannel	Grants permission to update a channel in a channel group	Write	Channel*		
			ChannelGroup*		
UpdateChannelGroup	Grants permission to update a channel group	Write	ChannelGroup*		
UpdateOriginEndpoint	Grants permission to update an origin endpoint of a channel	Write	Channel*		
			ChannelGroup*		
			OriginEndpoint*		

Resource types defined by AWS Elemental MediaPackage 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
ChannelGroup	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}	aws:ResourceTag/${TagKey}
ChannelPolicy	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}	
Channel	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}	aws:ResourceTag/${TagKey}
OriginEndpointPolicy	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}	
OriginEndpoint	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}	aws:ResourceTag/${TagKey}
HarvestJob	arn:${Partition}:mediapackagev2:${Region}:${Account}:channelGroup/${ChannelGroupName}/channel/${ChannelName}/originEndpoint/${OriginEndpointName}/harvestJob/${HarvestJobName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental MediaPackage V2

AWS Elemental MediaPackage V2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental MediaPackage VOD

AWS Elemental MediaPackage VOD (service prefix: `mediapackage-vod`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elemental MediaPackage VOD
- Resource types defined by AWS Elemental MediaPackage VOD
- Condition keys for AWS Elemental MediaPackage VOD

Actions defined by AWS Elemental MediaPackage VOD

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureLogs	Grants permission to configure egress access logs for a PackagingGroup	Write	packaging-groups*		iam:CreateServiceLinkedRole
CreateAsset	Grants permission to create an asset in AWS Elemental MediaPackage	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingConfiguration	Grants permission to create a packaging configuration in AWS Elemental MediaPackage	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackagingGroup	Grants permission to create a packaging group in AWS Elemental MediaPackage	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAsset	Grants permission to delete an asset in AWS Elemental MediaPackage	Write	assets*		
DeletePackagingConfiguration	Grants permission to delete a packaging configuration in AWS Elemental MediaPackage	Write	packaging-configurations*		
DeletePackagingGroup	Grants permission to delete a packaging group in AWS Elemental MediaPackage	Write	packaging-groups*		
DescribeAsset	Grants permission to view the details of an asset in AWS Elemental MediaPackage	Read	assets*		
DescribePackagingConfiguration	Grants permission to view the details of a packaging configuration in AWS Elemental MediaPackage	Read	packaging-configurations*		
DescribePackagingGroup	Grants permission to view the details of a packaging group in AWS Elemental MediaPackage	Read	packaging-groups*		
ListAssets	Grants permission to view a list of assets in AWS Elemental MediaPackage	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPackagingConfigurations	Grants permission to view a list of packaging configurations in AWS Elemental MediaPackage	List			
ListPackagingGroups	Grants permission to view a list of packaging groups in AWS Elemental MediaPackage	List			
ListTagsForResource	Grants permission to list the tags assigned to a Packaging Group, PackagingConfiguration, or Asset	Read	assets		
			packaging-configurations		
			packaging-groups		
TagResource	Grants permission to assign tags to a PackagingGroup, PackagingConfiguration, or Asset	Tagging	assets		
			packaging-configurations		
			packaging-groups		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to delete tags from a PackagingGroup, PackagingConfiguration, or Asset	Tagging	assets		
			packaging-configurations		
			packaging-groups		
				aws:TagKeys	
UpdatePackagingGroup	Grants permission to update a packaging group in AWS Elemental MediaPackage	Write	packaging-groups*		

Resource types defined by AWS Elemental MediaPackage VOD

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
assets	`arn:${Partition}:mediapackage-vod:${Region}:${Account}:assets/${AssetIdentifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
packaging-configurations	arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-configurations/${PackagingConfigurationIdentifier}	aws:ResourceTag/${TagKey}
packaging-groups	arn:${Partition}:mediapackage-vod:${Region}:${Account}:packaging-groups/${PackagingGroupIdentifier}	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental MediaPackage VOD

AWS Elemental MediaPackage VOD defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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 AWS Elemental MediaStore

AWS Elemental MediaStore (service prefix: `mediastore`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elemental MediaStore

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContainer	Grants permission to create a container	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteContainer	Grants permission to delete a container	Write	container*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContainerPolicy	Grants permission to delete the access policy of a container	Permissions management	container*		
DeleteCorsPolicy	Grants permission to delete the CORS policy from a container	Write	container*		
DeleteLifecyclePolicy	Grants permission to delete the lifecycle policy from a container	Write	container*		
DeleteMetricPolicy	Grants permission to delete the metric policy from a container	Write	container*		
DeleteObject	Grants permission to delete an object	Write	object*		
DescribeContainer	Grants permission to retrieve details on a container	List	container*		
DescribeObject	Grants permission to retrieve metadata for an object	List	object*		
GetContainerPolicy	Grants permission to retrieve the access policy of a container	Read	container*		
GetCorsPolicy	Grants permission to retrieve the CORS policy of a container	Read	container*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLifecyclePolicy	Grants permission to retrieve the lifecycle policy that is assigned to a container	Read	container*		
GetMetricPolicy	Grants permission to retrieve the metric policy that is assigned to a container	Read	container*		
GetObject	Grants permission to retrieve an object	Read	object*		
ListContainers	Grants permission to retrieve a list of containers in the current account	List			
ListItems	Grants permission to retrieve a list of objects and subfolders that are stored in a folder	List	folder		
ListTagsForResource	Grants permission to list tags on a container	Read	container		
PutContainerPolicy	Grants permission to create or replace the access policy of a container	Permissions management	container*		
PutCorsPolicy	Grants permission to add or modify the CORS policy of a container	Write	container*		
PutLifecyclePolicy	Grants permission to add or modify the lifecycle policy that is assigned to a container	Write	container*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricPolicy	Grants permission to add or modify the metric policy that is assigned to a container	Write	container*		
PutObject	Grants permission to upload an object	Write	object*		
StartAccessLogging	Grants permission to start access logging on a container	Write	container*		iam:PassRole
StopAccessLogging	Grants permission to stop access logging on a container	Write	container*		
TagResource	Grants permission to add tags to a container	Tagging	container		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a container	Tagging	container		
				aws:TagKeys	

Resource types defined by AWS Elemental MediaStore

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
container	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}`	aws:ResourceTag/${TagKey}
object	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${ObjectPath}`	
folder	`arn:${Partition}:mediastore:${Region}:${Account}:container/${ContainerName}/${FolderPath}`	

Condition keys for AWS Elemental MediaStore

AWS Elemental MediaStore defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental MediaTailor

AWS Elemental MediaTailor (service prefix: `mediatailor`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elemental MediaTailor

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureLogsForChannel	Grants permission to configure logs on the channel with the specified channel name	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfigureLogsForPlaybackConfiguration	Grants permission to configure logs for a playback configuration	Write	playbackConfiguration*		iam:CreateServiceLinkedRole
CreateChannel	Grants permission to create a new channel	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLiveSource	Grants permission to create a new live source on the source location with the specified source location name	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrefetchSchedule	Grants permission to create a prefetch schedule for the playback configuration with the specified playback configuration name	Write	playbackConfiguration*		
CreateProgram	Grants permission to create a new program on the channel with the specified channel name	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSourceLocation	Grants permission to create a new source location	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVodSource	Grants permission to create a new VOD source on the source location with the specified source location name	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Grants permission to delete the channel with the specified channel name	Write	channel*		
DeleteChannelPolicy	Grants permission to delete the IAM policy on the channel with the specified channel name	Permissions management	channel*		
DeleteLiveSource	Grants permission to delete the live source with the specified live source name on the source location with the specified source location name	Write	liveSource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePlaybackConfiguration	Grants permission to delete the specified playback configuration	Write	playbackConfiguration*		
DeletePrefetchSchedule	Grants permission to delete a prefetch schedule for a playback configuration with the specified prefetch schedule name	Write	playbackConfiguration*		
			prefetchSchedule*		
DeleteProgram	Grants permission to delete the program with the specified program name on the channel with the specified channel name	Write	program*		
DeleteSourceLocation	Grants permission to delete the source location with the specified source location name	Write	sourceLocation*		
DeleteVodSource	Grants permission to delete the VOD source with the specified VOD source name on the source location with the specified source location name	Write	vodSource*		
DescribeChannel	Grants permission to retrieve the channel with the specified channel name	Read	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLiveSource	Grants permission to retrieve the live source with the specified live source name on the source location with the specified source location name	Read	liveSource*		
DescribeProgram	Grants permission to retrieve the program with the specified program name on the channel with the specified channel name	Read	program*		
DescribeSourceLocation	Grants permission to retrieve the source location with the specified source location name	Read	sourceLocation*		
DescribeVodSource	Grants permission to retrieve the VOD source with the specified VOD source name on the source location with the specified source location name	Read	vodSource*		
GetChannelPolicy	Grants permission to read the IAM policy on the channel with the specified channel name	Read	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetChannelSchedule	Grants permission to retrieve the schedule of programs on the channel with the specified channel name	Read	channel*		
GetPlaybackConfiguration	Grants permission to retrieve the configuration for the specified name	Read	playbackConfiguration*		
GetPrefetchSchedule	Grants permission to retrieve prefetch schedule for a playback configuration with the specified prefetch schedule name	Read	playbackConfiguration*		
			prefetchSchedule*		
ListAlerts	Grants permission to retrieve the list of alerts on a resource	Read			
ListChannels	Grants permission to retrieve the list of existing channels	Read			
ListLiveSources	Grants permission to retrieve the list of existing live sources on the source location with the specified source location name	Read			
ListPlaybackConfigurations	Grants permission to retrieve the list of available configurations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrefetchSchedules	Grants permission to retrieve the list of prefetch schedules for a playback configuration	List	playbackConfiguration*		
ListSourceLocations	Grants permission to retrieve the list of existing source locations	Read			
ListTagsForResource	Grants permission to list the tags assigned to the specified playback configuration resource	Read	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
ListVodSources	Grants permission to retrieve the list of existing VOD sources on the source location with the specified source location name	Read			
PutChannelPolicy	Grants permission to set the IAM policy on the channel with the specified channel name	Permissions management	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPlaybackConfiguration	Grants permission to add a new configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StartChannel	Grants permission to start the channel with the specified channel name	Write	channel*		
StopChannel	Grants permission to stop the channel with the specified channel name	Write	channel*		
TagResource	Grants permission to add tags to the specified playback configuration resource	Tagging	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from the specified playback configuration resource	Tagging	channel		
			liveSource		
			playbackConfiguration		
			sourceLocation		
			vodSource		
				aws:TagKeys	
UpdateChannel	Grants permission to update the channel with the specified channel name	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLiveSource	Grants permission to update the live source with the specified live source name on the source location with the specified source location name	Write	liveSource*		
UpdateProgram	Grants permission to update the program with the specified program name on the channel with the specified channel name	Write	program*		
UpdateSourceLocation	Grants permission to update the source location with the specified source location name	Write	sourceLocation*		
UpdateVodSource	Grants permission to update the VOD source with the specified VOD source name on the source location with the specified source location name	Write	vodSource*		

Resource types defined by AWS Elemental MediaTailor

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
playbackConfiguration	arn:${Partition}:mediatailor:${Region}:${Account}:playbackConfiguration/${ResourceId}	aws:ResourceTag/${TagKey}
prefetchSchedule	arn:${Partition}:mediatailor:${Region}:${Account}:prefetchSchedule/${ResourceId}	
channel	arn:${Partition}:mediatailor:${Region}:${Account}:channel/${ChannelName}	aws:ResourceTag/${TagKey}
program	arn:${Partition}:mediatailor:${Region}:${Account}:program/${ChannelName}/${ProgramName}	
sourceLocation	arn:${Partition}:mediatailor:${Region}:${Account}:sourceLocation/${SourceLocationName}	aws:ResourceTag/${TagKey}
vodSource	arn:${Partition}:mediatailor:${Region}:${Account}:vodSource/${SourceLocationName}/${VodSourceName}	aws:ResourceTag/${TagKey}
liveSource	arn:${Partition}:mediatailor:${Region}:${Account}:liveSource/${SourceLocationName}/${LiveSourceName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental MediaTailor

AWS Elemental MediaTailor defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental Support Cases

AWS Elemental Support Cases (service prefix: `elemental-support-cases`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elemental Support Cases
- Resource types defined by AWS Elemental Support Cases
- Condition keys for AWS Elemental Support Cases

Actions defined by AWS Elemental Support Cases

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCaseComment [permission only]	Grants permission to add a comment to a support case	Write	case*		
CheckCasePermission [permission only]	Grants permission to verify whether the caller has the permissions to perform support case operations	Write			
CompleteMultipartUpload [permission only]	Grants permission to complete a multipart file upload to a support case	Write	case*		
CreateCase [permission only]	Grants permission to create a support case	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateS3CLIUploadCommand [permission only]	Grants permission to create a cli command to allow a file upload to a support case	Write	case*		
CreateS3DownloadUrl	Grants permission to download a file from a support case	Write	case*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
GetCase [permission only]	Grants permission to describe a support case in your account	Read	case*		
GetCasePermission [permission only]	Grants permission to verify whether the caller has the permissions to perform support case operations	Read			
GetCases [permission only]	Grants permission to list the support cases in your account	Read			
GetUICache [permission only]	Grants permission to retrieve cached case user data for use in the Console	Read			
ListTagsForCase [permission only]	Grants permission to list tags on a support case	Read	case*		
StartMultipartUpload [permission only]	Grants permission to start a multipart file upload to a support case	Write	case*		
TagCase [permission only]	Grants permission to add a tag on a support case	Tagging	case*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCase [permission only]	Grants permission to remove a tag on a support case	Tagging	case*		
				aws:TagKeys	
UpdateCase [permission only]	Grants permission to update a support case	Write	case*		
UpdateCaseStatus [permission only]	Grants permission to update a support case status	Write	case*		
UpdateMultipartUpload [permission only]	Grants permission to update a multipart file upload to a support case	Write	case*		

Resource types defined by AWS Elemental Support Cases

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
case	`arn:${Partition}:elemental-support-cases::${Account}:case/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Elemental Support Cases

AWS Elemental Support Cases defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elemental Support Content

AWS Elemental Support Content (service prefix: `elemental-support-content`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Elemental Support Content

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Query [permission only]	Grants permission to search support content	Read			

Resource types defined by AWS Elemental Support Content

AWS Elemental Support Content does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Elemental Support Content, specify `"Resource": "*"` in your policy.

Condition keys for AWS Elemental Support Content

Elemental Support Content has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon EMR on EKS (EMR Containers)

Amazon EMR on EKS (EMR Containers) (service prefix: `emr-containers`) 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 on EKS (EMR Containers)
- Resource types defined by Amazon EMR on EKS (EMR Containers)
- Condition keys for Amazon EMR on EKS (EMR Containers)

Actions defined by Amazon EMR on EKS (EMR Containers)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelJobRun	Grants permission to cancel a job run	Write	jobRun*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCertificate	Grants permission to call the CreateCertificate method to accept the CertificateSigning Request, and return the signed certificate	Write			
CreateJobTemplate	Grants permission to create a job template	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateManagedEndpoint	Grants permission to create a managed endpoint	Write	virtualCluster*		
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSecurityConfiguration	Grants permission to create a security configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateVirtualCluster	Grants permission to create a virtual cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteJobTemplate	Grants permission to delete a job template	Write	jobTemplate*		
DeleteManagedEndpoint	Grants permission to delete a managed endpoint	Write	managedEndpoint*		
DeleteSecurityConfiguration	Grants permission to delete a security configuration	Write	securityConfiguration*		
DeleteVirtualCluster	Grants permission to delete a virtual cluster	Write	virtualCluster*		
DescribeJobRun	Grants permission to describe a job run	Read	jobRun*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJobTemplate	Grants permission to describe a job template	Read	jobTemplate*		
DescribeManagedEndpoint	Grants permission to describe a managed endpoint	Read	managedEndpoint*		
DescribeSecurityConfiguration	Grants permission to describe a security configuration	Read	securityConfiguration*		
DescribeVirtualCluster	Grants permission to describe a virtual cluster	Read	virtualCluster*		
GetManagedEndpointSessionCredentials	Grants permission to generate a session token used to connect to a managed endpoint	Write	managedEndpoint*		
ListJobRuns	Grants permission to list job runs associated with a virtual cluster	List	virtualCluster*		
ListJobTemplates	Grants permission to list job templates	List			
ListManagedEndpoints	Grants permission to list managed endpoints associated with a virtual cluster	List	virtualCluster*		
ListSecurityConfigurations	Grants permission to list security configurations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for the specified resource	List	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		
ListVirtualClusters	Grants permission to list virtual clusters	List			
StartJobRun	Grants permission to start a job run	Write	virtualCluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys emr-containers:ExecutionRoleArn emr-containers:JobTemplateArn	
TagResource	Grants permission to tag the specified resource	Tagging	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		

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	jobRun		
			jobTemplate		
			managedEndpoint		
			securityConfiguration		
			virtualCluster		
				aws:TagKeys	

Resource types defined by Amazon EMR on EKS (EMR Containers)

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
virtualCluster	arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}	aws:ResourceTag/${TagKey}
jobRun	arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/jobruns/${JobRunId}	aws:ResourceTag/${TagKey}
jobTemplate	arn:${Partition}:emr-containers:${Region}:${Account}:/jobtemplates/${JobTemplateId}	aws:ResourceTag/${TagKey}
managedEndpoint	arn:${Partition}:emr-containers:${Region}:${Account}:/virtualclusters/${VirtualClusterId}/endpoints/${EndpointId}	aws:ResourceTag/${TagKey}
securityConfiguration	arn:${Partition}:emr-containers:${Region}:${Account}:/securityconfigurations/${SecurityConfigurationId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon EMR on EKS (EMR Containers)

Amazon EMR on EKS (EMR Containers) defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs present in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys present in the request	ArrayOfString
emr-containers:ExecutionRoleArn	Filters access by the execution role arn present in the request	ARN
emr-containers:JobTemplateArn	Filters access by the job template arn present in the request	ARN

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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
AccessSystemProfileLogs [permission only]	Grants permission to access system profile logs	Write	jobRun*		
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS End User Messaging SMS and Voice V2

AWS End User Messaging SMS and Voice V2 (service prefix: `sms-voice`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS End User Messaging SMS and Voice V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateOriginationIdentity	Grants permission to associate an origination phone number or sender ID to a pool	Write	Pool*		
			PhoneNumber		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SenderId		
AssociateProtectConfiguration	Grants permission to associate a protect configuration to a configuration set	Write	ConfigurationSet*		
			ProtectConfiguration*		
CreateConfigurationSet	Grants permission to create a configuration set	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateEventDestination	Grants permission to create an event destination within a configuration set	Write	ConfigurationSet*		iam:PassRole
CreateOptOutList	Grants permission to create an opt-out list	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreatePool	Grants permission to create a pool	Write	PhoneNumber		sms-voice:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SenderId		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectConfiguration	Grants permission to create a protect configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistration	Grants permission to create a registration	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationAssociation	Grants permission to associate a registration with a phone number or another registration	Write	Registration*		
			PhoneNumber		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRegistrationAttachment	Grants permission to create a registration attachment	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
CreateRegistrationVersion	Grants permission to create a registration version	Write	Registration*		
CreateVerifiedDestinationNumber	Grants permission to create a verified destination number	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
DeleteAccountDefaultProtectConfiguration	Grants permission to delete the account default protect configuration	Write			
DeleteConfigurationSet	Grants permission to delete a configuration set	Write	ConfigurationSet*		
DeleteDefaultMessageType	Grants permission to delete the default message type for a configuration set	Write	ConfigurationSet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDefaultSenderId	Grants permission to delete the default sender ID for a configuration set	Write	ConfigurationSet*		
DeleteEventDestination	Grants permission to delete an event destination within a configuration set	Write	ConfigurationSet*		
DeleteKeyword	Grants permission to delete a keyword for a pool or origination phone number	Write	PhoneNumber		
			Pool		
DeleteMediaMessageSpendLimitOverride	Grants permission to delete an override for your account's media messaging monthly spend limit	Write			
DeleteOptOutList	Grants permission to delete an opt-out list	Write	OptOutList*		
DeleteOptedOutNumber	Grants permission to delete a destination phone number from an opt-out list	Write	OptOutList*		
DeletePool	Grants permission to delete a pool	Write	Pool*		
DeleteProtectConfiguration	Grants permission to delete a protect configuration	Write	ProtectConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProtectConfigurationRuleSetNumberOverride	Grants permission to delete a phone number override for a protect configuration	Write	ProtectConfiguration*		
DeleteRegistration	Grants permission to delete a registration	Write	Registration*		
DeleteRegistrationAttachment	Grants permission to delete a registration attachment	Write	RegistrationAttachment*		
DeleteRegistrationFieldValue	Grants permission to delete an optional registration field value	Write	Registration*		
DeleteResourcePolicy	Grants permission to delete a resource policy	Permissions management	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
DeleteTextMessageSpendLimitOverride	Grants permission to delete an override for your account's text messaging monthly spend limit	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedDestinationNumber	Grants permission to delete a verified destination number	Write	VerifiedDestinationNumber*		
DeleteVoiceMessageSpendLimitOverride	Grants permission to delete an override for your account's voice messaging monthly spend limit	Write			
DescribeAccountAttributes	Grants permission to describe the attributes of your account	Read			
DescribeAccountLimits	Grants permission to describe the service quotas for your account	Read			
DescribeConfigurationSets	Grants permission to describe the configuration sets in your account	Read	ConfigurationSet		
DescribeKeywords	Grants permission to describe the keywords for a pool or origination phone number	Read	PhoneNumber		
			Pool		
DescribeOptOutLists	Grants permission to describe the opt-out lists in your account	Read	OptOutList		
DescribeOptedOutNumbers	Grants permission to describe the destination phone numbers in an opt-out list	Read	OptOutList*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePhoneNumbers	Grants permission to describe the origination phone numbers in your account	Read	PhoneNumber		
DescribePools	Grants permission to describe the pools in your account	Read	Pool		
DescribeProtectConfigurations	Grants permission to describe the protect configurations in your account	Read	ProtectConfiguration		
DescribeRegistrationAttachments	Grants permission to describe the registration attachments in your account	Read	RegistrationAttachment		
DescribeRegistrationFieldDefinitions	Grants permission to describe the field definitions for a given registration type	Read			
DescribeRegistrationFieldValues	Grants permission to describe the field values for a given registration	Read	Registration*		
DescribeRegistrationSectionDefinitions	Grants permission to describe the section definitions for a given registration type	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRegistrationTypeDefinitions	Grants permission to describe the registration types supported by the service	Read			
DescribeRegistrationVersions	Grants permission to describe the versions for a given registration	Read	Registration*		
DescribeRegistrations	Grants permission to describe the registrations in your account	Read	Registration		
DescribeSenderIds	Grants permission to describe the sender IDs in your account	Read	SenderId		
DescribeSpendLimits	Grants permission to describe the monthly spend limits for your account	Read			
DescribeVerifiedDestinationNumbers	Grants permission to describe the verified destination numbers in your account	Read	VerifiedDestinationNumber		
DisassociateOriginationIdentity	Grants permission to disassociate an origination phone number or sender ID from a pool	Write	Pool*		
			PhoneNumber		
			SenderId		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateProtectConfiguration	Grants permission to disassociate a protect configuration from a configuration set	Write	ConfigurationSet*		
			ProtectConfiguration*		
DiscardRegistrationVersion	Grants permission to discard the latest version of a given registration	Write	Registration*		
GetProtectConfigurationCountryRuleSet	Grants permission to get the country rule set for a protect configuration	Read	ProtectConfiguration*		
GetResourcePolicy	Grants permission to get a resource policy	Read	OptOutList		
			PhoneNumber		
			Pool		
			SenderId		
ListPoolOriginationIdentities	Grants permission to list all origination phone numbers and sender IDs associated to a pool	Read	Pool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProtectConfigurationRuleSetNumberOverrides	Grants permission to list all phone number overrides for a protect configuration	Read	ProtectConfiguration*		
ListRegistrationAssociations	Grants permission to list all resources associated to a registration	Read	Registration*		
ListTagsForResource	Grants permission to list the tags for a resource	Read	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VerifiedDestinationNumber		
PutKeyword	Grants permission to create or update a keyword for a pool or origination phone number	Write	PhoneNumber		
			Pool		
PutMessageFeedback	Grants permission to put feedback for a text, voice, or media message	Write	Message*		
PutOptedOutNumber	Grants permission to put a destination phone number into an opt-out list	Write	OptOutList*		
PutProtectConfigurationRuleSetNumberOverride	Grants permission to put a phone number override for a protect configuration	Write	ProtectConfiguration*		
PutRegistrationFieldValue	Grants permission to put a registration field value	Write	Registration*		
PutResourcePolicy	Grants permission to put a resource policy	Permissions management	OptOutList		
			PhoneNumber		
			Pool		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SenderId		
ReleasePhoneNumber	Grants permission to release an origination phone number	Write	PhoneNumber*		
ReleaseSenderId	Grants permission to release a sender ID	Write	SenderId*		
RequestPhoneNumber	Grants permission to request an origination phone number	Write	Pool		sms-voice:AssociateOriginationIdentity sms-voice:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RequestSenderId	Grants permission to request an unregistered sender ID	Write		aws:RequestTag/${TagKey} aws:TagKeys	sms-voice:TagResource
SendDestinationNumberVerificationCode	Grants permission to send a text or voice message containing a verification code to a destination phone number	Write	PhoneNumber		sms-voice:SendTextMessage sms-voice:SendVoiceMessage
			Pool		
			SenderId		
SendMediaMessage	Grants permission to send a media message to a destination phone number	Write	PhoneNumber		
			Pool		
SendTextMessage	Grants permission to send a text message to a destination phone number	Write	PhoneNumber		
			Pool		
			SenderId		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendVoiceMessage	Grants permission to send a voice message to a destination phone number	Write	PhoneNumber		
			Pool		
SetAccountDefaultProtectConfiguration	Grants permission to set a default protect configuration for the account	Write	ProtectConfiguration*		
SetDefaultMessageFeedbackEnabled	Grants permission to set the default message feedback for a configuration set	Write	ConfigurationSet*		
SetDefaultMessageType	Grants permission to set the default message type for a configuration set	Write	ConfigurationSet*		
SetDefaultSenderId	Grants permission to set the default sender ID for a configuration set	Write	ConfigurationSet*		
SetMediaMessageSpendLimitOverride	Grants permission to set an override for your account's media messaging monthly spend limit	Write			
SetTextMessageSpendLimitOverride	Grants permission to set an override for your account's text messaging monthly spend limit	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetVoiceMessageSpendLimitOverride	Grants permission to set an override for your account's voice messaging monthly spend limit	Write			
SubmitRegistrationVersion	Grants permission to submit the latest version of a given registration	Write	Registration*		
TagResource	Grants permission to add tags to a resource	Tagging	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		
			SenderId		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VerifiedDestinationNumber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	ConfigurationSet		
			OptOutList		
			PhoneNumber		
			Pool		
			ProtectConfiguration		
			Registration		
			RegistrationAttachment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SenderId		
			VerifiedDestinationNumber		
				aws:TagKeys	
UpdateEventDestination	Grants permission to update an event destination within a configuration set	Write	ConfigurationSet*		iam:PassRole
UpdatePhoneNumber	Grants permission to update an origination phone number's configuration	Write	PhoneNumber*		iam:PassRole
UpdatePool	Grants permission to update a pool's configuration	Write	Pool*		iam:PassRole
UpdateProtectConfiguration	Grants permission to update a protect configuration	Write	ProtectConfiguration*		
UpdateProtectConfigurationCountryRuleSet	Grants permission to update a country rule set for a protect configuration	Write	ProtectConfiguration*		
UpdateSenderId	Grants permission to update a sender ID's configuration	Write	SenderId*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
VerifyDestinationNumber	Grants permission to verify a destination phone number	Write	VerifiedDestinationNumber*		

Resource types defined by AWS End User Messaging SMS and Voice 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
ConfigurationSet	`arn:${Partition}:sms-voice:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
OptOutList	`arn:${Partition}:sms-voice:${Region}:${Account}:opt-out-list/${OptOutListName}`	aws:ResourceTag/${TagKey}
PhoneNumber	`arn:${Partition}:sms-voice:${Region}:${Account}:phone-number/${PhoneNumberId}`	aws:ResourceTag/${TagKey}
Pool	`arn:${Partition}:sms-voice:${Region}:${Account}:pool/${PoolId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ProtectConfiguration	arn:${Partition}:sms-voice:${Region}:${Account}:protect-configuration/${ProtectConfigurationId}	aws:ResourceTag/${TagKey}
SenderId	arn:${Partition}:sms-voice:${Region}:${Account}:sender-id/${SenderId}/${IsoCountryCode}	aws:ResourceTag/${TagKey}
Registration	arn:${Partition}:sms-voice:${Region}:${Account}:registration/${RegistrationId}	aws:ResourceTag/${TagKey}
RegistrationAttachment	arn:${Partition}:sms-voice:${Region}:${Account}:registration-attachment/${RegistrationAttachmentId}	aws:ResourceTag/${TagKey}
VerifiedDestinationNumber	arn:${Partition}:sms-voice:${Region}:${Account}:verified-destination-number/${VerifiedDestinationNumberId}	aws:ResourceTag/${TagKey}
Message	arn:${Partition}:sms-voice:${Region}:${Account}:message/${MessageId}	

Condition keys for AWS End User Messaging SMS and Voice V2

AWS End User Messaging SMS and Voice V2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS End User Messaging Social

AWS End User Messaging Social (service prefix: `social-messaging`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS End User Messaging Social
- Resource types defined by AWS End User Messaging Social
- Condition keys for AWS End User Messaging Social

Actions defined by AWS End User Messaging Social

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateWhatsAppBusinessAccount	Grants permission to associate a WhatsApp Business Account with your AWS account	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWhatsAppMessageTemplate	Grants permission to create a WhatsApp message template	Write	waba*		
CreateWhatsAppMessageTemplateFromLibrary	Grants permission to create a WhatsApp message template from Meta's template library	Write	waba*		
CreateWhatsAppMessageTemplateMedia	Grants permission to create media for WhatsApp message templates	Write	waba*		
DeleteWhatsAppMessageMedia	Grants permission to delete a media object from WhatsApp	Write	phone-number-id*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWhatsAppMessageTemplate	Grants permission to delete a WhatsApp message template	Write	waba*		
DisassociateWhatsAppBusinessAccount	Grants permission to disassociate a WhatsApp Business Account from your AWS account	Write	waba*		
GetLinkedWhatsAppBusinessAccount	Grants permission to view the details of a WhatsApp Business Account	Read	waba*		
GetLinkedWhatsAppBusinessAccountPhoneNumber	Grants permission to view the details of a phone number	Read	phone-number-id*		
GetWhatsAppMessageMedia	Grants permission to get a media object from WhatsApp	Write	phone-number-id*		
GetWhatsAppMessageTemplate	Grants permission to get details of a WhatsApp message template	Read	waba*		
ListLinkedWhatsAppBusinessAccounts	Grants permission to view all of your WhatsApp Business Accounts	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a resource	Read	phone-number-id		
			waba		
ListWhatsAppMessageTemplates	Grants permission to list WhatsApp message templates	List	waba*		
ListWhatsAppTemplateLibrary	Grants permission to list available templates from Meta's template library	List	waba*		
PostWhatsAppMessageMedia	Grants permission to upload a media object to WhatsApp	Write	phone-number-id*		
PutWhatsAppBusinessAccountEventDestinations	Grants permission to update a WhatsApp Business Accounts event destination	Write	waba*		
SendWhatsAppMessage	Grants permission to send a message through WhatsApp	Write	phone-number-id*		
TagResource	Grants permission to add a tag to a resource	Tagging	phone-number-id		
			waba		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag from a resource	Tagging	phone-number-id		
			waba		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateWhatsAppMessageTemplate	Grants permission to update a WhatsApp message template	Write	waba*		

Resource types defined by AWS End User Messaging Social

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
phone-number-id	`arn:${Partition}:social-messaging:${Region}:${Account}:phone-number-id/${OriginationPhoneNumberId}`	aws:ResourceTag/${TagKey}
waba	`arn:${Partition}:social-messaging:${Region}:${Account}:waba/${WabaId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS End User Messaging Social

AWS End User Messaging Social defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Entity Resolution

AWS Entity Resolution (service prefix: `entityresolution`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Entity Resolution

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPolicyStatement	Grants permission to give an AWS service or another account permission to use	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	an AWS Entity Resolution resources				
BatchDeleteUniqueId	Grants permission to batch delete unique Id	Write	MatchingWorkflow*		
CreateIdMappingWorkflow	Grants permission to create a idmapping workflow	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIdNamespace	Grants permission to create a IdNamespace	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMatchingWorkflow	Grants permission to create a matching workflow	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSchemaMapping	Grants permission to create a schema mapping	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdMappingWorkflow	Grants permission to delete a idmapping workflow	Write	IdMappingWorkflow*		
DeleteIdNamespace	Grants permission to delete a IdNamespace	Write	IdNamespace*		
DeleteMatchingWorkflow	Grants permission to delete a matching workflow	Write	MatchingWorkflow*		
DeletePolicyStatement	Grants permission to delete permission given to an AWS service or another account permission to use an AWS Entity Resolution resources	Permissions management			
DeleteSchemaMapping	Grants permission to delete a schema mapping	Write	SchemaMaping*		
GenerateMatchId	Grants permission to generate match Id	Write	MatchingWorkflow*		
GetIdMappingJob	Grants permission to get a idmapping job	Read	IdMappingWorkflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdMappingWorkflow	Grants permission to get a idmapping workflow	Read	IdMappingWorkflow*		
GetIdNamespace	Grants permission to get a IdNamespace	Read	IdNamespace*		
GetMatchId	Grants permission to get match Id	Read	MatchingWorkflow*		
GetMatchingJob	Grants permission to get a matching job	Read	MatchingWorkflow*		
GetMatchingWorkflow	Grants permission to get a matching workflow	Read	MatchingWorkflow*		
GetPolicy	Grants permission to get a resource policy for an AWS Entity Resolution resources	Read			
GetProviderService	Grants permission to get provider service	Read	ProviderService*		
GetSchemaMapping	Grants permission to get a schema mapping	Read	SchemaMapping*		
ListIdMappingJobs	Grants permission to list idmapping jobs	List	IdMappingWorkflow*		
ListIdMappingWorkflows	Grants permission to list idmapping workflows	List			
ListIdNamespaces	Grants permission to list IdNamespaces	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMatchingJobs	Grants permission to list matching jobs	List	MatchingWorkflow*		
ListMatchingWorkflows	Grants permission to list matching workflows	List			
ListProviderServices	Grants permission to list provider service	List			
ListSchemaMappings	Grants permission to list schema mappings	List			
ListTagsForResource	Grants permission to List tags for a resource	Read			
PutPolicy	Grants permission to put a resource policy for an AWS Entity Resolution resources	Permissions management			
StartIdMappingJob	Grants permission to start a idmapping job	Write	IdMappingWorkflow*		
StartMatchingJob	Grants permission to start a matching job	Write	MatchingWorkflow*		
TagResource	Grants permission to adds tags to a resource	Tagging	IdMappingWorkflow		
			IdNamespace		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	IdMappingWorkflow		
			IdNamespace		
			MatchingWorkflow		
			ProviderService		
			SchemaMapping		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIdMappingWorkflow	Grants permission to update a idmapping workflow	Write	IdMappingWorkflow*		
UpdateIdNamespace	Grants permission to update a IdNamespace	Write	IdNamespace*		
UpdateMatchingWorkflow	Grants permission to update a matching workflow	Write	MatchingWorkflow*		
UpdateSchemaMapping	Grants permission to update a schema mapping	Write	SchemaMapping*		
UseIdNamespace	Grants permission to give an AWS service or another account permission to use IdNamespace within a workflow	Permissions management			
UseWorkflow	Grants permission to give an AWS service or another account permission to use workflow within a IdNamespace	Permissions management			

Resource types defined by AWS Entity Resolution

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
MatchingWorkflow	arn:${Partition}:entityresolution:${Region}:${Account}:matchingworkflow/${WorkflowName}	aws:ResourceTag/${TagKey}
SchemaMapping	arn:${Partition}:entityresolution:${Region}:${Account}:schemamapping/${SchemaName}	aws:ResourceTag/${TagKey}
IdMappingWorkflow	arn:${Partition}:entityresolution:${Region}:${Account}:idmappingworkflow/${WorkflowName}	aws:ResourceTag/${TagKey}
ProviderService	arn:${Partition}:entityresolution:${Region}:${Account}:providerservice/${ProviderName}/${ProviderServiceName}	aws:ResourceTag/${TagKey}
IdNamespace	arn:${Partition}:entityresolution:${Region}:${Account}:idnamespace/${IdNamespaceName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Entity Resolution

AWS Entity Resolution defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the entity resolution service	String
aws:ResourceTag/${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 entity resolution service	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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateEventSource	Grants permission to activate partner event sources	Write	event-source*		
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for EventBridge	Write	event-bus*		
CancelReplay	Grants permission to cancel a replay	Write	replay*		
CreateApiDestination	Grants permission to create a new api destination	Write	api-destination*		
			connection*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribeRule	Grants permission to retrieve details about rules	Read	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListEventSources	Grants permission to to retrieve a list of event sources shared with this account	List			
ListPartnerEventSourceAccounts	Grants permission to retrieve a list of AWS account IDs associated with an event source	List	event-source*		
ListPartnerEventSources	Grants permission to retrieve a list partner event sources	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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	
PutPartnerEvents	Grants permission to sends custom events to Amazon EventBridge	Write			
PutPermission	Grants permission to use the PutPermission action to grants permission to another AWS account to put events to your default event bus	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutRule	Grants permission to create or updates rules	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTargets	Grants permission to add targets to a rule	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	Grants permission to revoke the permission of another AWS account to put events to your default event bus	Permissions management			
RemoveTargets	Grants permission to removes targets from a rule	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [permission only]	Grants permission to retrieve credentials from a connection	Write	connection*		
StartReplay	Grants permission to start a replay of an archive	Write	archive*		
			event-bus*		
			replay*		
TagResource	Grants permission to add a tag to an Amazon EventBridge resource	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	Grants permission to test whether an event pattern matches the provided event	Read			
UntagResource	Grants permission to remove a tag from an Amazon EventBridge resource	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApiDestination	Grants permission to update an api destination	Write	api-destination*		
UpdateArchive	Grants permission to update an archive	Write	archive*		
			alias		
			key		
UpdateConnection	Grants permission to update a connection	Write	connection*		
UpdateEndpoint	Grants permission to update an endpoint	Write	endpoint*		
				events:EventBusArn	
UpdateEventBus	Grants permission to update event buses	Write	event-bus*		

Resource types defined by Amazon EventBridge

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
event-source	`arn:${Partition}:events:${Region}::event-source/${EventSourceName}`	

Resource types	ARN	Condition keys
event-bus	arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}	aws:ResourceTag/${TagKey}
rule-on-default-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${RuleName}	aws:ResourceTag/${TagKey}
rule-on-custom-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}	aws:ResourceTag/${TagKey}
archive	arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}	
replay	arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}	
connection	arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}	
api-destination	arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}	
endpoint	arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}	
create-snapshot	arn:${Partition}:events:${Region}:${Account}:target/create-snapshot	
reboot-instance	arn:${Partition}:events:${Region}:${Account}:target/reboot-instance	
stop-instance	arn:${Partition}:events:${Region}:${Account}:target/stop-instance	

Resource types	ARN	Condition keys
terminate-instance	arn:${Partition}:events:${Region}:${Account}:target/terminate-instance	
alias	arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}	
key	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Condition keys for Amazon EventBridge

Amazon EventBridge defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags to event bus and rule actions	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource to event bus and rule actions	String
aws:TagKeys	Filters access by the tags in the request to event bus and rule actions	ArrayOfString
events:EventBusArn	Filters access by the ARN of the event buses that can be associated with an endpoint to CreateEndpoint and UpdateEndpoint actions	ArrayOfARN

Condition keys	Description	Type
events:ManagedBy	Filters access by AWS services. If a rule is created by an AWS service on your behalf, the value is the principal name of the service that created the rule	String
events:TargetArn	Filters access by the ARN of a target that can be put to a rule to PutTargets actions. TargetARN doesn't include DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	Filters access by the account the rule was created in to rule actions	String
events:detail-type	Filters access by the literal string of the detail-type of the event to PutEvents and PutRule actions	ArrayOfString
events:detail.eventTypeCode	Filters access by the literal string for the detail.eventTypeCode field of the event to PutRule actions	String
events:detail.service	Filters access by the literal string for the detail.service field of the event to PutRule actions	String
events:detail.userIdentity.principalId	Filters access by the literal string for the detail.useridentity.principalid field of the event to PutRule actions	String
events:eventBusInvocation	Filters access by whether the event was generated via API or cross-account bus invocation to PutEvents actions	String
events:source	Filters access by the AWS service or AWS partner event source that generated the event to PutEvents and PutRule actions. Matches the literal string of the source field of the event	ArrayOfString

Actions, resources, and condition keys for Amazon EventBridge Pipes

Amazon EventBridge Pipes (service prefix: `pipes`) 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 Pipes

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePipe	Grants permission to create a pipe	Write	pipe*		iam:PassRole
				aws:RequestTag/${TagKey} aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
DeletePipe	Grants permission to delete a pipe	Write	pipe*		
				aws:ResourceTag/${TagKey}	
DescribePipe	Grants permission to describe a pipe	Read	pipe*		
				aws:ResourceTag/${TagKey}	
ListPipes	Grants permission to list all pipes in your account	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	pipe*		
				aws:ResourceTag/${TagKey}	
StartPipe	Grants permission to start a pipe	Write	pipe*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
StopPipe	Grants permission to stop a pipe	Write	pipe*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to add tags to a resource	Tagging	pipe*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	pipe*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdatePipe	Grants permission to update a pipe	Write	pipe*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon EventBridge Pipes

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
pipe	`arn:${Partition}:pipes:${Region}:${Account}:pipe/${Name}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon EventBridge Pipes

Amazon EventBridge Pipes defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by allowed set of values for each of the tags	String
aws:ResourceTag/${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 EventBridge Scheduler

Amazon EventBridge Scheduler (service prefix: `scheduler`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EventBridge Scheduler

- Resource types defined by Amazon EventBridge Scheduler
- Condition keys for Amazon EventBridge Scheduler

Actions defined by Amazon EventBridge Scheduler

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSchedule	Grants permission to create an Amazon EventBridge Scheduler schedule	Write	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	
CreateScheduleGroup	Grants permission to create an Amazon EventBridge Scheduler schedule group	Write	schedule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSchedule	Grants permission to delete an Amazon EventBridge Scheduler schedule	Write	schedule*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
DeleteScheduleGroup	Grants permission to delete an Amazon EventBridge Scheduler schedule group	Write	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Grants permission to view details about an Amazon EventBridge Scheduler schedule	Read	schedule*		
				aws:ResourceTag/${TagKey}	
GetScheduleGroup	Grants permission to view details about an Amazon EventBridge Scheduler schedule group	Read	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	Grants permission to list the Amazon EventBridge Scheduler schedule groups in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSchedules	Grants permission to list the Amazon EventBridge Scheduler schedules in your account	List			
ListTagsForResource	Grants permission to lists tag for an Amazon EventBridge Scheduler resource	Read	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag an Amazon EventBridge Scheduler resource	Tagging	schedule-group*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an Amazon EventBridge Scheduler resource	Tagging	schedule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Grants permission to modify an Amazon EventBridge Scheduler schedule	Write	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon EventBridge Scheduler

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
schedule-group	`arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
schedule	arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}	

Condition keys for Amazon EventBridge Scheduler

Amazon EventBridge Scheduler defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon EventBridge Schemas

Amazon EventBridge Schemas (service prefix: schemas) 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 Schemas

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDiscoverer	Grants permission to create an event schema discoverer. Once created, your events will be automatically map into corresponding schema documents	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegistry	Grants permission to create a new schema registry in your account	Write	registry*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSchema	Grants permission to create a new schema in your account	Write	schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDiscoverer	Grants permission to delete discoverer in your account	Write	discoverer*		
DeleteRegistry	Grants permission to delete an existing registry in your account	Write	registry*		
DeleteResourcePolicy	Grants permission to delete the resource-based policy attached to a given registry	Write	registry*		
DeleteSchema	Grants permission to delete an existing schema in your account	Write	schema*		
DeleteSchemaVersion	Grants permission to delete a specific version of schema in your account	Write	schema*		
DescribeCodeBinding	Grants permission to retrieve metadata for generated code for specific schema in your account	Read	schema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDiscoverer	Grants permission to retrieve discoverer metadata in your account	Read	discoverer*		
DescribeRegistry	Grants permission to describe an existing registry metadata in your account	Read	registry*		
DescribeSchema	Grants permission to retrieve an existing schema in your account	Read	schema*		
ExportSchema	Grants permission to export the AWS registry or discovered schemas in OpenAPI 3 format to JSONSchema format	Read	registry* schema*		
GetCodeBindingSource	Grants permission to retrieve metadata for generated code for specific schema in your account	Read	schema*		
GetDiscoveredSchema	Grants permission to retrieve a schema for the provided list of sample events	Read			
GetResourcePolicy	Grants permission to retrieve the resource-based policy attached to a given registry	Read	registry*		
ListDiscoverers	Grants permission to list all discoverers in your account	List	discoverer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRegistries	Grants permission to list all registries in your account	List	registry*		
ListSchemaVersions	Grants permission to list all versions of a schema	List	schema*		
ListSchemas	Grants permission to list all schemas	List	schema*		
ListTagsForResource	Grants permission to lists tags for a resource	Read	discoverer		
			registry		
			schema		
PutCodeBinding	Grants permission to generate code for specific schema in your account	Write	schema*		
PutResourcePolicy	Grants permission to attach a resource-based policy to a given registry	Write	registry*		
SearchSchemas	Grants permission to search schemas based on specified keywords in your account	List	schema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDiscoverer	Grants permission to start the specified discoverer. Once started the discoverer will automatically register schemas for published events to configured source in your account	Write	discoverer*		
StopDiscoverer	Grants permission to stop the specified discoverer. Once stopped the discoverer will no longer register schemas for published events to configured source in your account	Write	discoverer*		
TagResource	Grants permission to tag a resource	Tagging	discoverer		
			registry		
			schema		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag from a resource	Tagging	discoverer		
			registry		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			schema		
				aws:TagKeys	
UpdateDiscoverer	Grants permission to update an existing discoverer in your account	Write	discoverer*		
UpdateRegistry	Grants permission to update an existing registry metadata in your account	Write	registry*		
UpdateSchema	Grants permission to update an existing schema in your account	Write	schema*		

Resource types defined by Amazon EventBridge Schemas

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
discoverer	`arn:${Partition}:schemas:${Region}:${Account}:discoverer/${DiscovererId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
registry	arn:${Partition}:schemas:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}
schema	arn:${Partition}:schemas:${Region}:${Account}:schema/${RegistryName}/${SchemaName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon EventBridge Schemas

Amazon EventBridge Schemas defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Fault Injection Service

AWS Fault Injection Service (service prefix: fis) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Fault Injection Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExperimentTemplate	Grants permission to create an AWS FIS experiment template	Write	action*		
			experiment-template*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateTargetAccountConfiguration	Grants permission to create an AWS FIS target account configuration	Write	experiment-template*		
DeleteExperimentTemplate	Grants permission to delete the AWS FIS experiment template	Write	experiment-template*		
DeleteTargetAccountConfiguration	Grants permission to delete an AWS FIS target account configuration	Write	experiment-template*		
GetAction	Grants permission to retrieve an AWS FIS action	Read	action*		
				aws:ResourceTag/${TagKey}	
GetExperiment	Grants permission to retrieve an AWS FIS experiment	Read	experiment*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExperimentTargetAccountConfiguration	Grants permission to retrieve an AWS FIS target account configuration for an AWS FIS experiment	Read	experiment*		
GetExperimentTemplate	Grants permission to retrieve an AWS FIS Experiment Template	Read	experiment-template*		
				aws:ResourceTag/${TagKey}	
GetSafetyLever	Grants permission to get information about the safety lever	Read	safety-lever*		
GetTargetAccountConfiguration	Grants permission to retrieve an AWS FIS target account configuration for an AWS FIS experiment template	Read	experiment-template*		
GetTargetResourceType	Grants permission to get information about the specified resource type	Read			
InjectApiInternalError [permission only]	Grants permission to inject an API internal error on the provided AWS service from an FIS Experiment	Write	experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fis:Service fis:Operations fis:Percentage fis:Targets	
InjectApiThrottleError [permission only]	Grants permission to inject an API throttle error on the provided AWS service from an FIS Experiment	Write	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InjectApiUnavailableError [permission only]	Grants permission to inject an API unavailable error on the provided AWS service from an FIS Experiment	Write	experiment*		
				fis:Service fis:Operations fis:Percentage fis:Targets	
ListActions	Grants permission to list all available AWS FIS actions	List			
ListExperimentResolvedTargets	Grants permission to list resolved targets for AWS FIS experiments	List	experiment*		
ListExperimentTargetAccountConfigurations	Grants permission to list target account configurations for AWS FIS experiments	List	experiment*		
ListExperimentTemplates	Grants permission to list all available AWS FIS experiment templates	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExperiments	Grants permission to list all available AWS FIS experiments	List			
ListTagsForResource	Grants permission to list the tags for an AWS FIS resource	Read	action		
			experiment		
			experiment-template		
ListTargetAccountConfigurations	Grants permission to list target account configurations for AWS FIS experiment templates	List	experiment-template*		
ListTargetResourceTypes	Grants permission to list the resource types	List			
StartExperiment	Grants permission to run an AWS FIS experiment	Write	experiment*		iam:CreateServiceLinkedRole
			experiment-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
StopExperiment	Grants permission to stop an AWS FIS experiment	Write	experiment*		
TagResource	Grants permission to tag AWS FIS resources	Tagging	action		
			experiment		
			experiment-template		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag AWS FIS resources	Tagging	action		
			experiment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			experiment-template		
				aws:TagKeys	
UpdateExperimentTemplate	Grants permission to update the specified AWS FIS experiment template	Write	experiment-template*		
			action		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSafetyLeverState	Grants permission to update the state of the safety lever	Write	safety-lever*		
UpdateTargetAccountConfiguration	Grants permission to update an AWS FIS target account configuration	Write	experiment-template*		

Resource types defined by AWS Fault Injection 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
action	`arn:${Partition}:fis:${Region}:${Account}:action/${Id}`	aws:ResourceTag/${TagKey}
experiment	`arn:${Partition}:fis:${Region}:${Account}:experiment/${Id}`	aws:ResourceTag/${TagKey}
experiment-template	`arn:${Partition}:fis:${Region}:${Account}:experiment-template/${Id}`	aws:ResourceTag/${TagKey}
safety-lever	`arn:${Partition}:fis:${Region}:${Account}:safety-lever/${Id}`	

Condition keys for AWS Fault Injection Service

AWS Fault Injection Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String

Condition keys	Description	Type
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
fis:Operations	Filters access by the list of operations on the AWS service that is being affected by the AWS FIS action	ArrayOfString
fis:Percentage	Filters access by the percentage of calls being affected by the AWS FIS action	Numeric
fis:Service	Filters access by the AWS service that is being affected by the AWS FIS action	String
fis:Targets	Filters access by the list of resource ARNs being targeted by the AWS FIS action	ArrayOfString

Actions, resources, and condition keys for Amazon FinSpace

Amazon FinSpace (service prefix: `finspace`) 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 FinSpace
- Resource types defined by Amazon FinSpace
- Condition keys for Amazon FinSpace

Actions defined by Amazon FinSpace

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConnectKxCluster [permission only]	Grants permission to connect to a kdb cluster	Write	kxCluster*		
CreateEnvironment	Grants permission to create a FinSpace environment	Write	environment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxChangeset	Grants permission to create a changeset for a kdb database	Write	kxDatabase*		
CreateKxCluster	Grants permission to create a cluster in a managed kdb environment	Write	kxCluster*		ec2:DescribeSubnets finspace:MountKxDatabase

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDatabase	Grants permission to create a kdb database in a managed kdb environment	Write	kxDatabase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxDataview	Grants permission to create a dataview in a managed kdb environment	Write	kxDataview*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKxEnvironment	Grants permission to create a managed kdb environment	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxScalingGroup	Grants permission to create a scaling group in a managed kdb environment	Write	kxScalingGroup*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxUser	Grants permission to create a user in a managed kdb environment	Write	kxEnvironment*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateKxVolume	Grants permission to create a volume in a managed kdb environment	Write	kxVolume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateUser	Grants permission to create a FinSpace user	Write	environment*		
			user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEnvironment	Grants permission to delete a FinSpace environment	Write	environment*		
DeleteKxCluster	Grants permission to delete a kdb cluster	Write	kxCluster*		
DeleteKxClusterNode	Grants permission to delete a node from a kdb cluster	Write	kxCluster*		
DeleteKxDatabase	Grants permission to delete a kdb database	Write	kxDatabase*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteKxDataview	Grants permission to delete a dataview in a managed kdb environment	Write	kxDataview*		
DeleteKxEnvironment	Grants permission to delete a managed kdb environment	Write	kxEnvironment*		
DeleteKxScalingGroup	Grants permission to delete a scaling group in a managed kdb environment	Write	kxScalingGroup*		
DeleteKxUser	Grants permission to delete a kdb user	Write	kxUser*		
DeleteKxVolume	Grants permission to delete a volume in a managed kdb environment	Write	kxVolume*		
GetEnvironment	Grants permission to describe a FinSpace environment	Read	environment*		
GetKxChangeset	Grants permission to describe a changeset for a kdb database	Read	kxDatabase*		
GetKxCluster	Grants permission to describe a cluster in a managed kdb environment	Read	kxCluster*		
GetKxConnectionString	Grants permission to retrieve a connection string for kdb clusters	Read	kxCluster*		finspace:ConnectKxCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetKxDatabase	Grants permission to describe a kdb database	Read	kxDatabase*		
GetKxDataview	Grants permission to describe a databiew in a managed kdb environment	Read	kxDataview*		
GetKxEnvironment	Grants permission to describe a managed kdb environment	Read	kxEnvironment*		
GetKxScalingGroup	Grants permission to describe a scaling group in a managed kdb environment	Read	kxScalingGroup*		
GetKxUser	Grants permission to describe a kdb user	Read	kxUser*		
GetKxVolume	Grants permission to describe a volume in a managed kdb environment	Read	kxVolume*		
GetLoadSampleDataSetGroupIntoEnvironmentStatus	Grants permission to request status of the loading of sample data bundle	Read	environment*		
GetUser	Grants permission to describe a FinSpace user	Read	environment*		
			user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEnvironments	Grants permission to list FinSpace environments in the AWS account	List	environment*		
ListKxChangesets	Grants permission to list changesets for a kdb database	List	kxDatabase*		
ListKxClusterNodes	Grants permission to list cluster nodes in a managed kdb environment	List	kxCluster*		
ListKxClusters	Grants permission to list clusters in a managed kdb environment	List	kxEnvironment*		
ListKxDatabases	Grants permission to list kdb databases in a managed kdb environment	List	kxEnvironment*		
ListKxDataviews	Grants permission to list dataviews in a database	List	kxDatabase*		
ListKxEnvironments	Grants permission to list managed kdb environments	List			
ListKxScalingGroups	Grants permission to list scaling groups in a managed kdb environment	List	kxEnvironment*		
ListKxUsers	Grants permission to list users in a managed kdb environment	List	kxEnvironment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListKxVolumes	Grants permission to list volumes in a managed kdb environment	List	kxEnvironment*		
ListTagsForResource	Grants permission to return a list of tags for a resource	List	environment*		
			kxCluster*		
			kxDatabase*		
			kxDataview*		
			kxEnvironment*		
			kxScalingGroup*		
			kxUser*		
			kxVolume*		
ListUsers	Grants permission to list FinSpace users in an environment	List	environment*		
			user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LoadSampleDataSetGroupIntoEnvironment	Grants permission to load sample data bundle into your FinSpace environment	Write	environment*		
MountKxDatabase [permission only]	Grants permission to mount a database to a kdb cluster	Write	kxDatabase*		
ResetUserPassword	Grants permission to reset the password for a FinSpace user	Write	environment*		
			user*		
TagResource	Grants permission to tag a resource	Tagging	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			kxVolume		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	environment		
			kxCluster		
			kxDatabase		
			kxDataview		
			kxEnvironment		
			kxScalingGroup		
			kxUser		
			kxVolume		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update a FinSpace environment	Write	environment*		
UpdateKxClusterCodeConfiguration	Grants permission to update code configuration for a cluster in a managed kdb environment	Write	kxCluster*		
UpdateKxClusterDatabases	Grants permission to update databases for a cluster in a managed kdb environment	Write	kxCluster*		
UpdateKxDatabase	Grants permission to update a kdb database	Write	kxDatabase*		
UpdateKxDataview	Grants permission to update a dataview in a managed kdb environment	Write	kxDataview*		
UpdateKxEnvironment	Grants permission to update a managed kdb environment	Write	kxEnvironment*		
UpdateKxEnvironmentNetwork	Grants permission to update the network for a managed kdb environment	Write	kxEnvironment*		
UpdateKxUser	Grants permission to update a kdb user	Write	kxUser*		
UpdateKxVolume	Grants permission to update a volume in a managed kdb environment	Write	kxVolume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUser	Grants permission to update a FinSpace user	Write	environment*		
			user*		

Resource types defined by Amazon FinSpace

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:${Partition}:finspace:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
user	`arn:${Partition}:finspace:${Region}:${Account}:user/${UserId}`	aws:ResourceTag/${TagKey}
kxEnvironment	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
kxUser	`arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxUser/${UserName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
kxCluster	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxCluster/${KxCluster}	aws:ResourceTag/${TagKey}
kxDatabase	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}	aws:ResourceTag/${TagKey}
kxScalingGroup	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxScalingGroup/${KxScalingGroup}	aws:ResourceTag/${TagKey}
kxDataview	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxDatabase/${KxDatabase}/kxDataview/${KxDataview}	aws:ResourceTag/${TagKey}
kxVolume	arn:${Partition}:finspace:${Region}:${Account}:kxEnvironment/${EnvironmentId}/kxVolume/${KxVolume}	aws:ResourceTag/${TagKey}

Condition keys for Amazon FinSpace

Amazon FinSpace defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 FinSpace API

Amazon FinSpace API (service prefix: `finspace-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 FinSpace API
- Resource types defined by Amazon FinSpace API
- Condition keys for Amazon FinSpace API

Actions defined by Amazon FinSpace API

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProgrammaticAccessCredentials	Grants permission to retrieve FinSpace programmatic access credentials	Read	credential*		

Resource types defined by Amazon FinSpace 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
credential	`arn:${Partition}:finspace-api:${Region}:${Account}:/credentials/programmatic`	

Condition keys for Amazon FinSpace API

FinSpace API has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Firewall Manager

AWS Firewall Manager (service prefix: `fms`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Firewall Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAdminAccount	Grants permission to set the AWS Firewall Manager administrator account and enables the service in all organization accounts	Write			
AssociateThirdPartyFirewall	Grants permission to set the Firewall Manager administrator as a tenant administrator of a third-party firewall service	Write			
BatchAssociateResource	Grants permission to associate resources to an AWS Firewall Manager resource set	Write	resource-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDisassociateResource	Grants permission to disassociate resources from an AWS Firewall Manager resource set	Write	resource-set*		
DeleteAppsList	Grants permission to permanently deletes an AWS Firewall Manager applications list	Write	applications-list*		
DeleteNotificationChannel	Grants permission to delete an AWS Firewall Manager association with the IAM role and the Amazon Simple Notification Service (SNS) topic that is used to notify the FM administrator about major FM events and errors across the organization	Write			
DeletePolicy	Grants permission to permanently delete an AWS Firewall Manager policy	Write	policy*		
				aws:ResourceTag/${TagKey}	
DeleteProtocolsList	Grants permission to permanently deletes an AWS Firewall Manager protocols list	Write	protocols-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourceSet	Grants permission to permanently delete an AWS Firewall Manager resource set	Write	resource-set*		
				aws:ResourceTag/${TagKey}	
DisassociateAdminAccount	Grants permission to disassociate the account that has been set as the AWS Firewall Manager administrator account and and disables the service in all organization accounts	Write			
DisassociateThirdPartyFirewall	Grants permission to disassociate a Firewall Manager administrator from a third-party firewall tenant	Write			
GetAdminAccount	Grants permission to return the AWS Organizations account that is associated with AWS Firewall Manager as the AWS Firewall Manager administrator	Read			
GetAdminScope	Grants permission to return information about the specified account's administrative scope	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAppsList	Grants permission to return information about the specified AWS Firewall Manager applications list	Read	applications-list*		
GetComplianceDetail	Grants permission to retrieve detailed compliance information about the specified member account. Details include resources that are in and out of compliance with the specified policy	Read	policy*		
GetNotificationChannel	Grants permission to retrieve information about the Amazon Simple Notification Service (SNS) topic that is used to record AWS Firewall Manager SNS logs	Read			
GetPolicy	Grants permission to retrieve information about the specified AWS Firewall Manager policy	Read	policy*		
GetProtectionStatus	Grants permission to retrieve policy-level attack summary information in the event of a potential DDoS attack	Read	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProtocolsList	Grants permission to return information about the specified AWS Firewall Manager protocols list	Read	protocols-list*		
GetResourceSet	Grants permission to retrieve information about the specified AWS Firewall Manager resource set	Read	resource-set*		
GetThirdPartyFirewallAssociationStatus	Grants permission to retrieve the onboarding status of a Firewall Manager administrator account to third-party firewall vendor tenant	Read			
GetViolationDetails	Grants permission to retrieve violations for a resource based on the specified AWS Firewall Manager policy and AWS account	Read	policy*		
ListAdminAccountsForOrganization	Grants permission to return a AdminAccounts object that lists the Firewall Manager administrators within the organization that are onboarded to Firewall Manager by Associate AdminAccount	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAdminsManagingAccount	Grants permission to list the accounts that are managing the specified AWS Organizations member account	List			
ListAppsLists	Grants permission to return an array of AppsListDataSummary objects	List			
ListComplianceStatus	Grants permission to retrieve an array of PolicyComplianceStatus objects in the response. Use PolicyComplianceStatus to get a summary of which member accounts are protected by the specified policy	List	policy*		
ListDiscoveredResources	Grants permission to retrieve an array of resources in the organization's accounts that are available to be associated with a resource set	List			
ListMemberAccounts	Grants permission to retrieve an array of member account ids if the caller is FMS admin account	List			
ListPolicies	Grants permission to retrieve an array of PolicySummary objects in the response	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProtocolsLists	Grants permission to return an array of ProtocolsListDataSummary objects	List			
ListResourceSetResources	Grants permission to retrieve an array of resources that are currently associated to a resource set	List	resource-set*		
ListResourceSets	Grants permission to retrieve an array of ResourceSetSummary objects	List			
ListTagsForResource	Grants permission to list Tags for a given resource	Read	policy*		
ListThirdPartyFirewallFirewallPolicies	Grants permission to retrieve a list of all of the third-party firewall policies that are associated with the third-party firewall administrator's account	List			
PutAdminAccount	Grants permission to create or update an Firewall Manager administrator account	Write			
PutAppsList	Grants permission to create an AWS Firewall Manager applications list	Write	applications-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
PutNotificationChannel	Grants permission to designate the IAM role and Amazon Simple Notification Service (SNS) topic that AWS Firewall Manager (FM) could use to notify the FM administrator about major FM events and errors across the organization	Write			
PutPolicy	Grants permission to create an AWS Firewall Manager policy	Write	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutProtocolsList	Grants permission to creates an AWS Firewall Manager protocols list	Write	protocols-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
PutResourceSet	Grants permission to create an AWS Firewall Manager resource set	Write	resource-set*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to add a Tag to a given resource	Tagging	applications-list		
			policy		
			protocols-list		
			resource-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a Tag from a given resource	Tagging	applications-list		
			policy		
			protocols-list		
			resource-set		
				aws:TagKeys	

Resource types defined by AWS Firewall 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:${Partition}:fms:${Region}:${Account}:policy/${Id}	aws:ResourceTag/${TagKey}
applications-list	arn:${Partition}:fms:${Region}:${Account}:applications-list/${Id}	aws:ResourceTag/${TagKey}
protocols-list	arn:${Partition}:fms:${Region}:${Account}:protocols-list/${Id}	aws:ResourceTag/${TagKey}
resource-set	arn:${Partition}:fms:${Region}:${Account}:resource-set/${Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS Firewall Manager

AWS Firewall Manager defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 Forecast

Amazon Forecast (service prefix: `forecast`) 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 Forecast

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutoPredictor	Grants permission to create an auto predictor	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Grants permission to create a dataset	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetGroup	Grants permission to create a dataset group	Write	datasetGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetImportJob	Grants permission to create a dataset import job	Write	datasetImportJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainability	Grants permission to create an explainability	Write	forecast*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExplainabilityExport	Grants permission to create an explainability export using an explainability resource	Write	explainability*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecast	Grants permission to create a forecast	Write	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastEndpoint [permission only]	Grants permission to create an endpoint using a Predictor resource	Write	predictor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateForecastExportJob	Grants permission to create a forecast export job using a forecast resource	Write	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMonitor	Grants permission to create an monitor using a Predictor resource	Write	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictor	Grants permission to create a predictor	Write	datasetGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePredictorBacktestExportJob	Grants permission to create a predictor backtest export job using a predictor	Write	predictor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfAnalysis	Grants permission to create a what-if analysis	Write	forecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecast	Grants permission to create a what-if forecast	Write	whatIfAnalysis*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWhatIfForecastExport	Grants permission to create a what-if forecast export using what-if forecast resources	Write	whatIfForecast*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Grants permission to delete a dataset	Write	dataset*		
DeleteDatasetGroup	Grants permission to delete a dataset group	Write	datasetGroup*		
DeleteDatasetImportJob	Grants permission to delete a dataset import job	Write	datasetImportJob*		
DeleteExplainability	Grants permission to delete an explainability	Write	explainability*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteExplainabilityExport	Grants permission to delete an explainability export	Write	explainabilityExport*		
DeleteForecast	Grants permission to delete a forecast	Write	forecast*		
DeleteForecastEndpoint [permission only]	Grants permission to delete an endpoint resource	Write	endpoint*		
DeleteForecastExportJob	Grants permission to delete a forecast export job	Write	forecastExport*		
DeleteMonitor	Grants permission to delete a monitor resource	Write	monitor*		
DeletePredictor	Grants permission to delete a predictor	Write	predictor*		
DeletePredictorBacktestExportJob	Grants permission to delete a predictor backtest export job	Write	predictorBacktestExportJob*		
DeleteResourceTree	Grants permission to delete a resource and its child resources	Write	dataset*		
			datasetGroup*		
			datasetImportJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWhatIfAnalysis	Grants permission to delete a what-if analysis	Write	whatIfAnalysis*		
DeleteWhatIfForecast	Grants permission to delete a what-if forecast	Write	whatIfForecast*		
DeleteWhatIfForecastExport	Grants permission to delete a what-if forecast export	Write	whatIfForecastExport*		
DescribeAutoPredictor	Grants permission to describe an auto predictor	Read	predictor*		
DescribeDataset	Grants permission to describe a dataset	Read	dataset*		
DescribeDatasetGroup	Grants permission to describe a dataset group	Read	datasetGroup*		
DescribeDatasetImportJob	Grants permission to describe a dataset import job	Read	datasetImportJob*		
DescribeExplainability	Grants permission to describe an explainability	Read	explainability*		
DescribeExplainabilityExport	Grants permission to describe an explainability export	Read	explainabilityExport*		
DescribeForecast	Grants permission to describe a forecast	Read	forecast*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeForecastEndpoint [permission only]	Grants permission to describe an endpoint resource	Read	endpoint*		
DescribeForecastExportJob	Grants permission to describe a forecast export job	Read	forecastExport*		
DescribeMonitor	Grants permission to describe an monitor resource	Read	monitor*		
DescribePredictor	Grants permission to describe a predictor	Read	predictor*		
DescribePredictorBacktestExportJob	Grants permission to describe a predictor backtest export job	Read	predictorBacktestExportJob*		
DescribeWhatIfAnalysis	Grants permission to describe a what-if analysis	Read	whatIfAnalysis*		
DescribeWhatIfForecast	Grants permission to describe a what-if forecast	Read	whatIfForecast*		
DescribeWhatIfForecastExport	Grants permission to describe a what-if forecast export	Read	whatIfForecastExport*		
GetAccuracyMetrics	Grants permission to get the Accuracy Metrics for a predictor	Read	predictor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRecentForecastContext [permission only]	Grants permission to get the forecast context of a timeseries for an endpoint	Read	endpoint*		
InvokeForecastEndpoint [permission only]	Grants permission to invoke the endpoint to get forecast for a timeseries	Read	endpoint*		
ListDatasetGroups	Grants permission to list all the dataset groups	Read			
ListDatasetImportJobs	Grants permission to list all the dataset import jobs	Read			
ListDatasets	Grants permission to list all the datasets	Read			
ListExplainabilities	Grants permission to list all the explainabilities	Read			
ListExplainabilityExports	Grants permission to list all the explainability exports	Read			
ListForecastExportJobs	Grants permission to list all the forecast export jobs	Read			
ListForecasts	Grants permission to list all the forecasts	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMonitorEvaluations	Grants permission to list all the monitor evaluation result for a monitor	Read	monitor*		
ListMonitors	Grants permission to list all the monitor resources	Read			
ListPredictorBacktestExportJobs	Grants permission to list all the predictor backtest export jobs	Read			
ListPredictors	Grants permission to list all the predictors	Read			
ListTagsForResource	Grants permission to list the tags for an Amazon Forecast resource	Read	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
ListWhatIfAnalyses	Grants permission to list all the what-if analyses	Read			
ListWhatIfForecastExports	Grants permission to list all the what-if forecast exports	Read			
ListWhatIfForecasts	Grants permission to list all the what-if forecasts	Read			
QueryForecast	Grants permission to retrieve a forecast for a single item	Read	forecast*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
QueryWhatIfForecast	Grants permission to retrieve a what-if forecast for a single item	Read	whatIfForecast*		
ResumeResource	Grants permission to resume Amazon Forecast resource jobs	Write	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopResource	Grants permission to stop Amazon Forecast resource jobs	Write	datasetImportJob*		
			endpoint*		
			explainability*		
			explainabilityExport*		
			forecast*		
			forecastExport*		
			monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			predictor*		
			predictorBacktestExportJob*		
			whatIfAnalysis*		
			whatIfForecast*		
			whatIfForecastExport*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to associate the specified tags to a resource	Tagging	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to delete the specified tags for a resource	Tagging	dataset		
			datasetGroup		
			datasetImportJob		
			endpoint		
			explainability		
			explainabilityExport		
			forecast		
			forecastExport		
			monitor		
			predictor		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			predictorBacktestExportJob		
			whatIfAnalysis		
			whatIfForecast		
			whatIfForecastExport		
				aws:TagKeys	
UpdateDatasetGroup	Grants permission to update a dataset group	Write	dataset*		
			datasetGroup*		

Resource types defined by Amazon Forecast

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
dataset	arn:${Partition}:forecast:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}
datasetGroup	arn:${Partition}:forecast:${Region}:${Account}:dataset-group/${ResourceId}	aws:ResourceTag/${TagKey}
datasetImportJob	arn:${Partition}:forecast:${Region}:${Account}:dataset-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
algorithm	arn:${Partition}:forecast:::algorithm/${ResourceId}	
predictor	arn:${Partition}:forecast:${Region}:${Account}:predictor/${ResourceId}	aws:ResourceTag/${TagKey}
predictorBacktestExportJob	arn:${Partition}:forecast:${Region}:${Account}:predictor-backtest-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
forecast	arn:${Partition}:forecast:${Region}:${Account}:forecast/${ResourceId}	aws:ResourceTag/${TagKey}
forecastExport	arn:${Partition}:forecast:${Region}:${Account}:forecast-export-job/${ResourceId}	aws:ResourceTag/${TagKey}
explainability	arn:${Partition}:forecast:${Region}:${Account}:explainability/${ResourceId}	aws:ResourceTag/${TagKey}
explainabilityExport	arn:${Partition}:forecast:${Region}:${Account}:explainability-export/${ResourceId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
monitor	arn:${Partition}:forecast:${Region}:${Account}:monitor/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfAnalysis	arn:${Partition}:forecast:${Region}:${Account}:what-if-analysis/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfForecast	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast/${ResourceId}	aws:ResourceTag/${TagKey}
whatIfForecastExport	arn:${Partition}:forecast:${Region}:${Account}:what-if-forecast-export/${ResourceId}	aws:ResourceTag/${TagKey}
endpoint	arn:${Partition}:forecast:${Region}:${Account}:forecast-endpoint/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Forecast

Amazon Forecast defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Fraud Detector

Amazon Fraud Detector (service prefix: `frauddetector`) 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 Fraud Detector
- Resource types defined by Amazon Fraud Detector
- Condition keys for Amazon Fraud Detector

Actions defined by Amazon Fraud Detector

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateVariable	Grants permission to create a batch of variables	Write		aws:RequestTag/${TagKey} aws:TagKeys	
BatchGetVariable	Grants permission to get a batch of variables	List	variable*		
CancelBatchImportJob	Grants permission to cancel the specified batch import job	Write	batch-import*		
CancelBatchPredictionJob	Grants permission to cancel the specified batch prediction job	Write	batch-prediction*		
CreateBatchImportJob	Grants permission to create a batch import job	Write	batch-import*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBatchPredictionJob	Grants permission to create a batch prediction job	Write	batch-prediction*		
			detector*		
			detector-version*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorVersion	Grants permission to create a detector version. The detector version starts in a DRAFT status	Write	detector*		
			external-model		
			model-version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateList	Grants permission to create a list	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Grants permission to create a model using the specified model type	Write	event-type*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateModelVersion	Grants permission to create a version of the model using the specified model type and model id	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRule	Grants permission to create a rule for use with the specified detector	Write	detector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVariable	Grants permission to create a variable	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBatchImportJob	Grants permission to delete a batch import job	Write	batch-import*		
DeleteBatchPredictionJob	Grants permission to delete a batch prediction job	Write	batch-prediction*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDetector	Grants permission to delete the detector. Before deleting a detector, you must first delete all detector versions and rule versions associated with the detector	Write	detector*		
DeleteDetectorVersion	Grants permission to delete the detector version. You cannot delete detector versions that are in ACTIVE status	Write	detector-version*		
DeleteEntityType	Grants permission to delete an entity type. You cannot delete an entity type that is included in an event type	Write	entity-type*		
DeleteEvent	Grants permission to deletes the specified event	Write	event-type*		
DeleteEventType	Grants permission to delete an event type. You cannot delete an event type that is used in a detector or a model	Write	event-type*		
DeleteEventsByEventType	Grants permission to delete events for the specified event type	Write	event-type*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteExternalModel	Grants permission to remove a SageMaker model from Amazon Fraud Detector. You can remove an Amazon SageMaker model if it is not associated with a detector version	Write	external-model*		
DeleteLabel	Grants permission to delete a label. You cannot delete labels that are included in an event type in Amazon Fraud Detector. You cannot delete a label assigned to an event ID. You must first delete the relevant event ID	Write	label*		
DeleteList	Grants permission to delete a list	Write	list*		
				aws:ResourceTag/${TagKey}	
DeleteModel	Grants permission to delete a model. You can delete models and model versions in Amazon Fraud Detector, provided that they are not associated with a detector version	Write	model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelVersion	Grants permission to delete a model version. You can delete models and model versions in Amazon Fraud Detector, provided that they are not associated with a detector version	Write	model-version*		
DeleteOutcome	Grants permission to delete an outcome. You cannot delete an outcome that is used in a rule version	Write	outcome*		
DeleteRule	Grants permission to delete the rule. You cannot delete a rule if it is used by an ACTIVE or INACTIVE detector version	Write	rule*		
DeleteVariable	Grants permission to delete a variable. You cannot delete variables that are included in an event type in Amazon Fraud Detector	Write	variable*		
DescribeDetector	Grants permission to get all versions for a specified detector	Read	detector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelVersions	Grants permission to get all of the model versions for the specified model type or for the specified model type and model ID. You can also get details for a single, specified model version	Read	model-version		
GetBatchImportJobValidationReport [permission only]	Grants permission to get the data validation report of a specific batch import job	Read	batch-import*		
GetBatchImportJobs	Grants permission to get all batch import jobs or a specific job if you specify a job ID	List	batch-import		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBatchPredictionJobs	Grants permission to get all batch prediction jobs or a specific job if you specify a job ID. This is a paginated API. If you provide a null maxResults, this action retrieves a maximum of 50 records per page. If you provide a maxResults, the value must be between 1 and 50. To get the next page results, provide the pagination token from the GetBatchPredictionJobsResponse as part of your request. A null pagination token fetches the records from the beginning	List	batch-prediction		
GetDeleteEventsByEventTypeStatus	Grants permission to get a specific event type DeleteEventsByEventType API execution status	Read	event-type*		
GetDetectorVersion	Grants permission to get a particular detector version	Read	detector-version*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDetectors	Grants permission to get all detectors or a single detector if a detectorId is specified . This is a paginated API. If you provide a null maxResults, this action retrieves a maximum of 10 records per page. If you provide a maxResults, the value must be between 5 and 10. To get the next page results, provide the pagination token from the GetDetectorsResponse as part of your request. A null pagination token fetches the records from the beginning	List	detector		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEntityTypes	Grants permission to get all entity types or a specific entity type if a name is specified. This is a paginated API. If you provide a null maxResults, this action retrieves a maximum of 10 records per page. If you provide a maxResults, the value must be between 5 and 10. To get the next page results, provide the pagination token from the GetEntityTypesResponse as part of your request. A null pagination token fetches the records from the beginning	List	entity-type		
GetEvent	Grants permission to get the details of the specified event	Read	event-type*		
GetEventPrediction	Grants permission to evaluate an event against a detector version. If a version ID is not provided, the detector's (ACTIVE) version is used	Read	detector*		
			detector-version*		
			event-type*		
GetEventPredictionMetadata	Grants permission to get more details of a particular prediction	Read	detector*		
			detector-version*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			event-type*		
GetEventTypes	Grants permission to get all event types or a specific event type if name is provided. This is a paginated API. If you provide a null maxResults, this action retrieves a maximum of 10 records per page. If you provide a maxResults, the value must be between 5 and 10. To get the next page results, provide the pagination token from the GetEventTypesResponse as part of your request. A null pagination token fetches the records from the beginning	List	event-type		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExternalModels	Grants permission to get the details for one or more Amazon SageMaker models that have been imported into the service. This is a paginated API. If you provide a null maxResults, this actions retrieves a maximum of 10 records per page. If you provide a maxResults, the value must be between 5 and 10. To get the next page results, provide the pagination token from the GetExternalModelsResult as part of your request. A null pagination token fetches the records from the beginning	List	external-model		
GetKMSEncryptionKey	Grants permission to get the encryption key if a Key Management Service (KMS) customer master key (CMK) has been specified to be used to encrypt content in Amazon Fraud Detector	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLabels	Grants permission to get all labels or a specific label if name is provided. This is a paginated API. If you provide a null maxResults, this action retrieves a maximum of 50 records per page. If you provide a maxResults, the value must be between 10 and 50. To get the next page results, provide the paginatio n token from the GetGetLab elsResponse as part of your request. A null pagination token fetches the records from the beginning	List	label		
GetListEl ements	Grants permission to get elements of a list	Read	list*		
				aws:Resou rceTag/ ${ TagKey}	
GetListsM etadata	Grants permission to get metadata about lists	List	list		
				aws:Resou rceTag/ ${ TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetModelVersion	Grants permission to get the details of the specified model version	Read	model-version*		
GetModels	Grants permission to get one or more models. Gets all models for the AWS account if no model type and no model id provided. Gets all models for the AWS account and model type, if the model type is specified but model id is not provided. Gets a specific model if (model type, model id) tuple is specified	List	model		
GetOutcomes	Grants permission to get one or more outcomes. This is a paginated API. If you provide a null maxResults, this actions retrieves a maximum of 100 records per page. If you provide a maxResults, the value must be between 50 and 100. To get the next page results, provide the pagination token from the GetOutcomesResult as part of your request. A null pagination token fetches the records from the beginning	List	outcome		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRules	Grants permission to get all rules for a detector (paginated) if ruleId and ruleVersion are not specified. Gets all rules for the detector and the ruleId if present (paginated). Gets a specific rule if both the ruleId and the ruleVersion are specified	List	rule		
GetVariables	Grants permission to get all of the variables or the specific variable. This is a paginated API. Providing null maxSizePerPage results in retrieving maximum of 100 records per page. If you provide maxSizePerPage the value must be between 50 and 100. To get the next page result, a provide a pagination token from GetVariablesResult as part of your request. Null pagination token fetches the records from the beginning	List	variable		
ListEventPredictions	Grants permission to get a list of past predictions	List	detector		
			detector-version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			event-type		
ListTagsForResource	Grants permission to list all tags associated with the resource. This is a paginated API. To get the next page results, provide the pagination token from the response as part of your request. A null pagination token fetches the records from the beginning	Read	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rule		
			variable		
PutDetector	Grants permission to create or update a detector	Write	detector*		
			event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutEntityType	Grants permission to create or update an entity type. An entity represents who is performing the event. As part of a fraud prediction, you pass the entity ID to indicate the specific entity who performed the event. An entity type classifies the entity. Example classifications include customer, merchant, or account	Write	entity-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEventType	Grants permission to create or update an event type. An event is a business activity that is evaluated for fraud risk. With Amazon Fraud Detector, you generate fraud predictions for events. An event type defines the structure for an event sent to Amazon Fraud Detector. This includes the variables sent as part of the event, the entity performing the event (such as a customer), and the labels that classify the event. Example event types include online payment transactions, account registrations, and authentications	Write	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutExternalModel	Grants permission to create or update an Amazon SageMaker model endpoint. You can also use this action to update the configuration of the model endpoint, including the IAM role and/or the mapped variables	Write	event-type*		
			external-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutKMSEncryptionKey	Grants permission to specify the Key Management Service (KMS) customer master key (CMK) to be used to encrypt content in Amazon Fraud Detector	Write			
PutLabel	Grants permission to create or update label. A label classifies an event as fraudulent or legitimate. Labels are associated with event types and used to train supervised machine learning models in Amazon Fraud Detector	Write	label*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutOutcome	Grants permission to create or update an outcome	Write	outcome*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
SendEvent	Grants permission to send event	Write	event-type*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to assign tags to a resource	Tagging	batch-import		
			batch-prediction		
			detector		
			detector-version		
			entity-type		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	batch-import		
			batch-prediction		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			detector		
			detector-version		
			entity-type		
			event-type		
			external-model		
			label		
			list		
			model		
			model-version		
			outcome		
			rule		
			variable		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDetectorVersion	Grants permission to update a detector version. The detector version attributes that you can update include models, external model endpoints, rules, rule execution mode, and description. You can only update a DRAFT detector version	Write	detector*		
			external-model		
			model-version		
UpdateDetectorVersionMetadata	Grants permission to update the detector version's description. You can update the metadata for any detector version (DRAFT, ACTIVE, or INACTIVE)	Write	detector-version*		
UpdateDetectorVersionStatus	Grants permission to update the detector version's status. You can perform the following promotions or demotions using UpdateDetectorVersionStatus: DRAFT to ACTIVE, ACTIVE to INACTIVE, and INACTIVE to ACTIVE	Write	detector-version*		
UpdateEventLabel	Grants permission to update an existing event record's label value	Write	event-type*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateList	Grants permission to update a list	Write	list*		
				aws:ResourceTag/${TagKey}	
UpdateModel	Grants permission to update a model. You can update the description attribute using this action	Write	model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateModelVersion	Grants permission to update a model version. Updating a model version retrains an existing model version using updated training data and produces a new minor version of the model. You can update the training data set location and data access role attributes using this action. This action creates and trains a new minor version of the model, for example version 1.01, 1.02, 1.03	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateModelVersionStatus	Grants permission to update the status of a model version	Write	model-version*		
UpdateRuleMetadata	Grants permission to update a rule's metadata. The description attribute can be updated	Write	rule*		
UpdateRuleVersion	Grants permission to update a rule version resulting in a new rule version. Updates a rule version resulting in a new rule version (version 1, 2, 3 ...)	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVariable	Grants permission to update a variable	Write	variable*		

Resource types defined by Amazon Fraud Detector

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
batch-prediction	`arn:${Partition}:frauddetector:${Region}:${Account}:batch-prediction/${ResourcePath}`	aws:ResourceTag/${TagKey}
detector	`arn:${Partition}:frauddetector:${Region}:${Account}:detector/${ResourcePath}`	aws:ResourceTag/${TagKey}
detector-version	`arn:${Partition}:frauddetector:${Region}:${Account}:detector-version/${ResourcePath}`	aws:ResourceTag/${TagKey}
entity-type	`arn:${Partition}:frauddetector:${Region}:${Account}:entity-type/${ResourcePath}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
external-model	arn:${Partition}:frauddetector:${Region}:${Account}:external-model/${ResourcePath}	aws:ResourceTag/${TagKey}
event-type	arn:${Partition}:frauddetector:${Region}:${Account}:event-type/${ResourcePath}	aws:ResourceTag/${TagKey}
label	arn:${Partition}:frauddetector:${Region}:${Account}:label/${ResourcePath}	aws:ResourceTag/${TagKey}
model	arn:${Partition}:frauddetector:${Region}:${Account}:model/${ResourcePath}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:frauddetector:${Region}:${Account}:model-version/${ResourcePath}	aws:ResourceTag/${TagKey}
outcome	arn:${Partition}:frauddetector:${Region}:${Account}:outcome/${ResourcePath}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:frauddetector:${Region}:${Account}:rule/${ResourcePath}	aws:ResourceTag/${TagKey}
variable	arn:${Partition}:frauddetector:${Region}:${Account}:variable/${ResourcePath}	aws:ResourceTag/${TagKey}
batch-import	arn:${Partition}:frauddetector:${Region}:${Account}:batch-import/${ResourcePath}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
list	arn:${Partition}:frauddetector:${Region}:${Account}:list/${ResourcePath}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Fraud Detector

Amazon Fraud Detector defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the tags that are passed in the request	String
aws:ResourceTag/${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

Actions, resources, and condition keys for AWS Free Tier

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountActivity	Grants permission to get a specific activity record	Read			
GetAccountPlanState	Grants permission to get all of the information related to the state of the account plan related to Free Tier	Read			
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
ListAccountActivities	Grants permission to list available activities	List			
PutFreeTierAlertPreference [permission only]	Grants permission to set free tier alert preference (email address)	Write			
UpgradeAccountPlan	Grants permission to trigger an upgrade of account plan	Write			

Resource types defined by AWS Free Tier

AWS Free Tier does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Free Tier, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 for FreeRTOS extended maintenance plan (EMP)	Read	subscription*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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
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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFileGateway [permission only]	Grants permission to associate a File Gateway instance with an Amazon FSx for Windows File Server file system	Write	file-system*		
AssociateFileSystemAliases	Grants permission to associate DNS aliases with an Amazon FSx for Windows File Server file system	Write	file-system*		
BypassSnaplockEnterpriseRetention [permission only]	Grants permission to allow deletion of an FSx for ONTAP SnapLock Enterprise volume that contains WORM (write once, read many) files with active retention periods	Permissions management	volume*		
CancelDataRepositoryTask	Grants permission to cancel a data repository task	Write	task*		
CopyBackup	Grants permission to copy a backup	Write	backup*		fsx:TagResource
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${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*		
CreateAndAttachS3AccessPoint	Grants permission to create and attach a S3 Access Point to a FSx File System	Write	volume		s3:CreateAccessPoint s3:GetAccessPoint s3:PutAccessPointPolicy
CreateBackup	Grants permission to create a new backup of an Amazon FSx file system or an Amazon FSx volume	Write	backup*		fsx:TagResource
			file-system		
			volume		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryAssociation	Grants permission to create a new data respository association for an Amazon FSx for Lustre file system	Write	association*	fsx:NfsDataRepositoryAuthenticationEnabled fsx:NfsDataRepositoryEncryptionInTransitEnabled	fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataRepositoryTask	Grants permission to create a new data respository task for an Amazon FSx for Lustre file system	Write	file-system*		fsx:TagResource
			task*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFileCache	Grants permission to create a new, empty, Amazon file cache	Write	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	Grants permission to create a new, empty, Amazon FSx file system	Write	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	Grants permission to create a new Amazon FSx file system from an existing backup	Write	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Grants permission to create a new snapshot on a volume	Write	snapshot*		fsx:TagResource
			volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageVirtualMachine	Grants permission to create a new storage virtual machine in an Amazon FSx for Ontap file system	Write	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	Grants permission to create a new volume	Write	volume*		fsx:TagResource
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	Grants permission to create a new volume from backup	Write	backup*		fsx:TagResource
			storage-virtual-machine*		
			volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	
DeleteBackup	Grants permission to delete a backup, deleting its contents. After deletion, the backup no longer exists, and its data is no longer available	Write	backup*		
DeleteDataRepositoryAssociation	Grants permission to delete a data repository association	Write	association*		
DeleteFileCache	Grants permission to delete a file cache, deleting its contents	Write	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFileSystem	Grants permission to delete a file system, deleting its contents and any existing automatic backups of the file system	Write	file-system*		fsx:CreateBackup fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [permission only]	Grants permission to manage cross-account sharing of FSx volumes through AWS Resource Access Manager (RAM). PutResourcePolicy and GetResourcePolicy are also required	Permissions management	volume*		
DeleteSnapshot	Grants permission to delete a snapshot on a volume	Write	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStorageVirtualMachine	Grants permission to delete a storage virtual machine, deleting its contents	Write	storage-virtual-machine*		
DeleteVolume	Grants permission to delete a volume, deleting its contents and any existing automatic backups of the volume	Write	volume*		fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [permission only]	Grants permission to describe the File Gateway instances associated with an Amazon FSx for Windows File Server file system	Read	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBackups	Grants permission to return the descriptions of all backups owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeDataRepositoryAssociations	Grants permission to return the descriptions of all data repository associations owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeDataRepositoryTasks	Grants permission to return the descriptions of all data repository tasks owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeFileCaches	Grants permission to return the descriptions of all file caches owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFileSystemAliases	Grants permission to return the description of all DNS aliases owned by your Amazon FSx for Windows File Server file system	Read	file-system*		
DescribeFileSystems	Grants permission to return the descriptions of all file systems owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeS3AccessPointAttachments	Grants permission to return the descriptions of S3 Access Point Attachments	Read			
DescribeSharedVpcConfiguration	Grants permission to return the descriptions of whether FSx route table updates from participant accounts are allowed in your account	Read			
DescribeSnapshots	Grants permission to return the descriptions of all snapshots owned by your AWS account in the AWS Region of the endpoint you're calling	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStorageVirtualMachines	Grants permission to return the descriptions of all storage virtual machines owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeVolumes	Grants permission to return the descriptions of all volumes owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DetachAndDeleteS3AccessPoint	Grants permission to detach an S3 Access Point from an Amazon FSx File System and delete the S3 Access Point	Write	volume		s3:DeleteAccessPoint
DisassociateFileGateway [permission only]	Grants permission to disassociate a File Gateway instance from an Amazon FSx for Windows File Server file system	Write	file-system*		
DisassociateFileSystemAliases	Grants permission to disassociate file system aliases with an Amazon FSx for Windows File Server file system	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy [permission only]	Grants permission to manage cross-account sharing of FSx volumes through AWS Resource Access Manager (RAM). PutResourcePolicy and DeleteResourcePolicy are also required	Permissions management	volume*		
ListTagsForResource	Grants permission to list tags for an Amazon FSx resource	Read	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ManageBackupPrincipalAssociations [permission only]	Grants permission to manage backup principal associations through AWS Backup	Permissions management	backup*		
PutResourcePolicy [permission only]	Grants permission to manage cross-account sharing of FSx volumes through AWS Resource Access Manager (RAM). DeleteResourcePolicy and GetResourcePolicy are also required	Permissions management	volume*		
ReleaseFileSystemNfsV3Locks	Grants permission to release file system NFS V3 locks	Write	file-system*		
RestoreVolumeFromSnapshot	Grants permission to restore volume state from a snapshot	Write	snapshot* volume*		
StartMisconfiguredStateRecovery	Grants permission to start misconfigured state recovery	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an Amazon FSx resource	Tagging	association	fsx:NfsDataRepositoryAuthenticationEnabled fsx:NfsDataRepositoryEncryptionInTransitEnabled	
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	fsx:ParentVolumeId fsx:StorageVirtualMachineId	
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag from an Amazon FSx resource	Tagging	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume		
				aws:TagKeys	
UpdateDataRepositoryAssociation	Grants permission to update data repository association configuration	Write	association*		
UpdateFileCache	Grants permission to update file cache configuration	Write	file-cache*		
UpdateFileSystem	Grants permission to update file system configuration	Write	file-system*		
UpdateSharedVpcConfiguration	Grants permission to enable or disable FSx route table updates from participant accounts in your account	Write			
UpdateSnapshot	Grants permission to update snapshot configuration	Write	snapshot*		
UpdateStorageVirtualMachine	Grants permission to update storage virtual machine configuration	Write	storage-virtual-machine*		
UpdateVolume	Grants permission to update volume configuration	Write	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Resource types defined by Amazon FSx

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

> **Note**
>
> Amazon FSx for Windows File Server, Lustre, and Ontap share some of the same resource types, with the same ARN format for each.

Resource types	ARN	Condition keys
file-system	`arn:${Partition}:fsx:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
file-cache	`arn:${Partition}:fsx:${Region}:${Account}:file-cache/${FileCacheId}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
storage-virtual-machine	arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}	aws:ResourceTag/${TagKey}
task	arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}
association	arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}	aws:ResourceTag/${TagKey}
volume	arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon FSx

Amazon FSx defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
fsx:IsBackupCopyDestination	Filters access by whether the backup is a destination backup for a CopyBackup operation	Bool
fsx:IsBackupCopySource	Filters access by whether the backup is a source backup for a CopyBackup operation	Bool
fsx:NfsDataRepositoryAuthenticationEnabled	Filters access by NFS data repositories which support authentication	Bool
fsx:NfsDataRepositoryEncryptionInTransitEnabled	Filters access by NFS data repositories which support encryption-in-transit	Bool
fsx:ParentVolumeId	Filters access by the containing parent volume for mutating volume operations	String
fsx:StorageVirtualMachineId	Filters access by the containing storage virtual machine for a volume for mutating volume operations	String

Actions, resources, and condition keys for Amazon GameLift Servers

Amazon GameLift Servers (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 Servers

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	gamelift:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
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	containerFleet		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 AWS 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*		
GetPlayerConnectionDetails	Grants permission to retrieve player connection endpoints and player gateway tokens for a game session	Read			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCompute	Grants permission to retrieve all compute resources in the current Region	List	containerFleet		
			fleet		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGameServers	Grants permission to retrieve all game servers that are currently running in a game server group	List	gameServerGroup*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			matchmakingConfiguration		
			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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchGameSessions	Grants permission to retrieve game sessions that match a set of search criteria	Read			
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 Servers

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 Servers

Amazon GameLift Servers defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon GameLift Streams

Amazon GameLift Streams (service prefix: `gameliftstreams`) 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 Streams

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddStreamGroupLocations	Grants permission to attach a StreamGroup remote location	Write	streamgroup*		ec2:DescribeRegions
AssociateApplications	Grants permission to associate Applications to a StreamGroup	Write	application*		
			streamgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create application	Write		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource s3:GetObject s3:ListBucket
CreateStreamGroup	Grants permission to create a StreamGroup	Write		aws:RequestTag/${TagKey} aws:TagKeys	gameliftstreams:TagResource
CreateStreamSessionConnection	Grants permission to create a stream session connection	Write	stream group*		
DeleteApplication	Grants permission to delete an application	Write	application*		
DeleteStreamGroup	Grants permission to delete a StreamGroup	Write	stream group*		
DisassociateApplications	Grants permission to disassociate Applications from a StreamGroup	Write	application* stream group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportStreamSessionFiles	Grants permission to export stream session files that your application generates	Write	stream group*		s3:PutObject
GetApplication	Grants permission to get an application	Read	application*		
GetStreamGroup	Grants `permission` to get a StreamGroup	Read	stream group*		
GetStreamSession	Grants permission to get a stream session	Read	stream group*		
ListApplications	Grants permission to list applications	List			
ListStreamGroups	Grants permission to list StreamGroups	List			
ListStreamSessions	Grants permission to list stream sessions	Read	stream group*		
ListStreamSessionsByAccount	Grants permission to list stream sessions	Read			
ListTagsForResource	Grants permission to list tags for a resource	Read	application		
			stream group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveStreamGroupLocations	Grants permission to detach a StreamGroup remote location	Write	stream group*		
StartStreamSession	Grants permission to create a stream session	Write	stream group*		
TagResource	Grants permission to tag a resource	Tagging	application		
			stream group		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateStreamSession	Grants permission to terminate a stream session	Write	stream group*		
UntagResource	Grants permission to untag a resource	Tagging	application		
			stream group		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplication	Grants permission to update an application	Write	application*		
UpdateStreamGroup	Grants permission to update a StreamGroup	Write	streamgroup*		

Resource types defined by Amazon GameLift 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
application	`arn:${Partition}:gameliftstreams:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
streamgroup	`arn:${Partition}:gameliftstreams:${Region}:${Account}:streamgroup/${StreamGroupId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon GameLift Streams

Amazon GameLift Streams defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Global Accelerator

AWS Global Accelerator (service prefix: `globalaccelerator`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Global Accelerator
- Resource types defined by AWS Global Accelerator
- Condition keys for AWS Global Accelerator

Actions defined by AWS Global Accelerator

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCustomRoutingEndpoints	Grants permission to add a virtual private cloud (VPC) subnet endpoint to a custom routing accelerator endpoint group	Write	endpointgroup*		
AddEndpoints	Grants permission to add an endpoint to a standard accelerator endpoint group	Write	endpointgroup*		globalaccelerator:UpdateEndpointGroup
AdvertiseByoipCidr	Grants permission to advertises an IPv4 address range that is provisioned for use with your accelerator through bring your own IP addresses (BYOIP)	Write			
AllowCustomRoutingTraffic	Grants permission to allows custom routing of user traffic to a private destination IP:PORT in a specific VPC subnet	Write	endpointgroup*		
CreateAccelerator	Grants permission to create a standard accelerator	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCrossAccountAttachment	Grants permission to create a CrossAccountAttachment	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingAccelerator	Grants permission to create a Custom Routing accelerator	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomRoutingEndpointGroup	Grants permission to create an endpoint group for the specified listener for a custom routing accelerator	Write	listener*		
CreateCustomRoutingListener	Grants permission to create a listener to process inbound connections from clients to a custom routing accelerator	Write	accelerator*		
CreateEndpointGroup	Grants permission to add an endpoint group to a standard accelerator listener	Write	listener*		
CreateListener	Grants permission to add a listener to a standard accelerator	Write	accelerator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccelerator	Grants permission to delete a standard accelerator	Write	accelerator*		
DeleteCrossAccountAttachment	Grants permission to delete a CrossAccountAttachment	Write	attachment*		
DeleteCustomRoutingAccelerator	Grants permission to delete a custom routing accelerator	Write	accelerator*		
DeleteCustomRoutingEndpointGroup	Grants permission to delete an endpoint group from a listener for a custom routing accelerator	Write	endpointgroup*		
DeleteCustomRoutingListener	Grants permission to delete a listener for a custom routing accelerator	Write	listener*		
DeleteEndpointGroup	Grants permission to delete an endpoint group associated with a standard accelerator listener	Write	endpointgroup*		
DeleteListener	Grants permission to delete a listener from a standard accelerator	Write	listener*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DenyCustomRoutingTraffic	Grants permission to disallows custom routing of user traffic to a private destination IP:PORT in a specific VPC subnet	Write	endpointgroup*		
DeprovisionByoipCidr	Grants permission to releases the specified address range that you provisioned for use with your accelerator through bring your own IP addresses (BYOIP)	Write			
DescribeAccelerator	Grants permissions to describe a standard accelerator	Read	accelerator*		
DescribeAcceleratorAttributes	Grants permission to describe a standard accelerator attributes	Read	accelerator*		
DescribeCrossAccountAttachment	Grants permissions to describe a CrossAccountAttachment	Read	attachment*		
DescribeCustomRoutingAccelerator	Grants permission to describe a custom routing accelerator	Read	accelerator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCustomRoutingAcceleratorAttributes	Grants permission to describe the attributes of a custom routing accelerator	Read	accelerator*		
DescribeCustomRoutingEndpointGroup	Grants permission to describe an endpoint group for a custom routing accelerator	Read	endpointgroup*		
DescribeCustomRoutingListener	Grants permission to describe a listener for a custom routing accelerator	Read	listener*		
DescribeEndpointGroup	Grants permission to describe a standard accelerator endpoint group	Read	endpointgroup*		
DescribeListener	Grants permission to describe a standard accelerator listener	Read	listener*		
ListAccelerators	Grants permission to list all standard accelerators	List			
ListByoipCidrs	Grants permission to list the BYOIP cidrs	List			
ListCrossAccountAttachments	Grants permission to list all CrossAccountAttachments	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCrossAccountResourceAccounts	Grants permission to list accounts with CrossAccountAttachments listing caller as a principal	List			
ListCrossAccountResources	Grants permission to list all CrossAccountAttachment resources usable by caller	List			
ListCustomRoutingAccelerators	Grants permission to list the custom routing accelerators for an AWS account	List			
ListCustomRoutingEndpointGroups	Grants permission to list the endpoint groups that are associated with a listener for a custom routing accelerator	List	listener*		
ListCustomRoutingListeners	Grants permission to list the listeners for a custom routing accelerator	List	accelerator*		
ListCustomRoutingPortMappings	Grants permission to list the port mappings for a custom routing accelerator	List	accelerator*		
ListCustomRoutingPortMappingsByDestination	Grants permission to list the port mappings for a specific endpoint IP address (a destination address) in a subnet	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEndpointGroups	Grants permission to list all endpoint groups associated with a standard accelerator listener	List	listener*		
ListListeners	Grants permission to list all listeners associated with a standard accelerator	List	accelerator*		
ListTagsForResource	Grants permission to list tags for a globalaccelerator resource	Read	accelerator		
			attachment		
ProvisionByoipCidr	Grants permission to provisions an address range for use with your accelerator through bring your own IP addresses (BYOIP)	Write			
RemoveCustomRoutingEndpoints	Grants permission to remove virtual private cloud (VPC) subnet endpoints from a custom routing accelerator endpoint group	Write	endpointgroup*		
RemoveEndpoints	Grants permission to remove an endpoint from a standard accelerator endpoint group	Write	endpointgroup*		globalaccelerator:UpdateEndpointGroup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a globalaccelerator resource	Tagging	accelerator		
			attachment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a globalaccelerator resource	Tagging	accelerator		
			attachment		
				aws:TagKeys	
UpdateAccelerator	Grants permission to update a standard accelerator	Write	accelerator*		
UpdateAcceleratorAttributes	Grants permission to update a standard accelerator attributes	Write	accelerator*		
UpdateCrossAccountAttachment	Grants permission to update a CrossAccountAttachment	Write	attachment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCustomRoutingAccelerator	Grants permission to update a custom routing accelerator	Write	accelerator*		
UpdateCustomRoutingAcceleratorAttributes	Grants permission to update the attributes for a custom routing accelerator	Write	accelerator*		
UpdateCustomRoutingListener	Grants permission to update a listener for a custom routing accelerator	Write	listener*		
UpdateEndpointGroup	Grants permission to update an endpoint group on a standard accelerator listener	Write	endpointgroup*		
UpdateListener	Grants permission to update a listener on a standard accelerator	Write	listener*		
WithdrawByoipCidr	Grants permission to stops advertising a BYOIP IPv4 address	Write			

Resource types defined by AWS Global Accelerator

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
accelerator	arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}	aws:ResourceTag/${TagKey}
listener	arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}	aws:ResourceTag/${TagKey}
endpointgroup	arn:${Partition}:globalaccelerator::${Account}:accelerator/${ResourceId}/listener/${ListenerId}/endpoint-group/${EndpointGroupId}	aws:ResourceTag/${TagKey}
attachment	arn:${Partition}:globalaccelerator::${Account}:attachment/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Global Accelerator

AWS Global Accelerator defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Glue

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeInboundIntegration [permission only]	Grants permission to Glue to continuously validate that the target Arn can receive data replicated from the source ARN	Write	integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreatePartition	Grants permission to create one or more partitions	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
BatchDeleteConnection	Grants permission to delete one or more connections	Write	connection*		
			rootcatalog*		
				glue:LakeFormationPermissions	
BatchDeletePartition	Grants permission to delete one or more partitions	Write	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions	
BatchDeleteTable	Grants permission to delete one or more tables	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
BatchDeleteTableVersion	Grants permission to delete one or more versions of a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetBlueprints	Grants permission to retrieve one or more blueprints	Read	blueprint*		
BatchGetCrawlers	Grants permission to retrieve one or more crawlers	Read	crawler*		
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		
				glue:LakeFormationPermissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions	
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*		
CheckSchemaVersionValidity	Grants permission to retrieve a check the validity of schema version	Read			
CreateBlueprint	Grants permission to create a blueprint	Write	blueprint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	Grants permission to create a catalog	Write	catalog* rootcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
CreateClassifier	Grants permission to create a classifier	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateColumnStatisticsTaskSettings	Grants permission to create settings for a column statistics task	Write	database*		
			rootcatalog*		
			table*		
CreateConnection	Grants permission to create a connection	Write	rootcatalog*		
			connectionType		
				aws:RequestTag/${TagKey} aws:TagKeys glue:LakeFormationPermissions	
CreateCrawler	Grants permission to create a crawler	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
			rootcatalog*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
CreateDevEndpoint	Grants permission to create a development endpoint	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlueIdentityCenterConfiguration	Grants permission to connect Glue with Identity Center	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationResourceProperty	Grants permission to create integration resource property	Write	catalog*		
			connection*		
			database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integrationResourcePropertyarn*		
				aws:RequestTag/${TagKey} aws:TagKeys	
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
				glue:LakeFormationPermissions	
CreatePartitionIndex	Grants permission to create a specified partition index in an existing table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	Grants permission to create a script	Write			
CreateSecurityConfiguration	Grants permission to create a security configuration	Write			
CreateSession	Grants permission to create an interactive session	Write	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTable	Grants permission to create a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
			catalog		
				glue:LakeFormationPermissions	
CreateWorkflow	Grants permission to create a workflow	Write	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBlueprint	Grants permission to delete a blueprint	Write	blueprint*		
DeleteCatalog	Grants permission to delete a catalog	Write	rootcatalog*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
DeleteClassifier	Grants permission to delete a classifier	Write			
DeleteColumnStatisticsForPartition	Grants permission to delete the partition column statistics of a column	Write	database*		
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeleteColumnStatisticsForTable	Grants permission to delete the table statistics of columns	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions	
DeleteConnectionType	Grants permission to delete connection type	Write	connectionType*		
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*		
			table*		
			userdefinedfunction*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
DeleteDevEndpoint	Grants permission to delete a development endpoint	Write	devendpoint*		
DeleteGlueIdentityCenterConfiguration	Grants permission to disconnect Glue with Identity Center	Write			
DeleteIntegration	Grants permission to delete an integration	Write	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationResourceProperty	Grants permission to delete the integration resource property	Write	catalog*		
			connection*		
			database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integrationResourceProperty*		
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*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeletePartitionIndex	Grants permission to delete a specified partition index from an existing table	Write	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
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		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
DeleteTrigger	Grants permission to delete a trigger	Write	trigger*		
DeleteUsageProfile	Grants permission to delete a usage profile	Write	usageProfile*		
DeleteUserDefinedFunction	Grants permission to delete a function definition	Write	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
				glue:LakeFormationPermissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	Permissions management	connectionType		
DescribeEntity	Grants permission to describe entity in glue studio	Permissions management	connection*		
			rootcatalog*		
			connectionType		
DescribeInboundIntegrations	Grants permission to list the inbound integrations	List			
DescribeIntegrations	Grants permission to describe zero-ETL integrations	List	integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
FederateAuthorization	Grants permission to read and write redshift federated resources	Write	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery glue:FederatedAuthorizationSource	
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:EnabledForRedshiftAutoDiscovery glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetCatalogImportStatus	Grants permission to retrieve the catalog import status	Read	rootcatalog*		
				glue:LakeFormationPermissions	
GetCatalogs	Grants permission to retrieve all catalogs	Read	rootcatalog*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:EnabledForRedshiftAutoDiscovery glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
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		
				glue:LakeFormationPermissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetColumnStatisticsForTable	Grants permission to retrieve table statistics of columns	Read	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
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 AWS Q	Read	completion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConnection	Grants permission to retrieve a connection	Read	connection*		
			rootcatalog*		
				glue:LakeFormationPermissions	
GetConnections	Grants permission to retrieve a list of connections	Read	connection*		
			rootcatalog*		
				glue:LakeFormationPermissions	
GetCrawler	Grants permission to retrieve a crawler	Read	crawler*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetDataQualityResult	Grants permission to retrieve a Data Quality result	Read	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	Grants permission to retrieve a Data Quality rule recommendation run	Read	dataQualityRuleset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetDatabases	Grants permission to retrieve all databases	Read	database*		
			rootcatalog*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
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		
			connectionType		
GetEnvironment	Grants permission to get environment details for SparkUI	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetGlueIdentityCenterConfiguration	Grants permission to retrieve the managed Idc application	Read			
GetIntegrationResourceProperty	Grants permission to retrieve the integration resource property	Read	catalog*		
			connection*		
			database*		
			integrationResourceProperty*		
GetIntegrationTableProperties	Grants permission to retrieve the integration table properties	Read	catalog*		
			connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				glue:LakeFormationPermissions	
GetPartitionIndexes	Grants permission to retrieve partition indexes for a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions	
GetPartitions	Grants permission to retrieve the partitions of a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetTableOptimizer	Grants permission to return the configuration of all optimizers associated with a specified table	Read	database*		glue:GetTable
			rootcatalog*		
			table*		
GetTableVersion	Grants permission to retrieve a version of a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetTableVersions	Grants permission to retrieve a list of versions of a table	Read	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
GetTables	Grants permission to retrieve the tables in a database	Read	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
GetTags	Grants permission to retrieve all tags associated with a resource	Read	blueprint		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			connection		
			connectionType		
			crawler		
			customEntityType		
			database		
			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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserDefinedFunction	Grants permission to retrieve a function definition	Read	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
				glue:LakeFormationPermissions	
GetUserDefinedFunctions	Grants permission to retrieve multiple function definitions	Read	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
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 AWS Glue	Write	rootcatalog*		
				glue:LakeFormationPermissions	
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	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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataQualityRuleRecommendationRuns	Grants permission to retrieve all Data Quality rule recommendation runs	List	dataQualityRuleset*		
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*		
			connectionType		
ListIntegrationResourceProperties	Grants permission to list zero-ETL integration resource properties	List	catalog*		
			connection*		
			database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integrationResourceProperty*		
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
			connectionType		
RegisterConnectionType	Grants permission to register connection type	Write	connectionType*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RegisterSchemaVersion	Grants permission to create a new schema version	Write	registry*		
			schema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveSchemaVersionMetadata	Grants permission to remove metadata from schema version	Write	registry		
			schema		
RenameTable	Grants permission to rename a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				glue:LakeFormationPermissions	
SendFeedback	Grants permission to provide feedback about a glue completion experience in AWS Q	Write			
SendRecipeAction	Grants permission to execute a Data Preparation Recipe statement in data preview	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Q experience	Write			
StartCrawler	Grants permission to start a crawler	Write	crawler*		
StartCrawlerSchedule	Grants permission to change the schedule state of a crawler to SCHEDULED	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
StartMLLabelingSetGenerationTaskRun	Grants permission to start a Labeling Set Generation ML Task Run	Write	mlTransform*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
StopCrawlerSchedule	Grants permission to set the schedule state of a crawler to NOT_SCHEDULED	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			catalog		
			connection		
			connectionType		
			crawler		
			customEntityType		
			dataQualityRuleset		
			database		
			devendpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integration		
			integrationResourceProperty		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} glue:LakeFormationPermissions	
TerminateNotebook	Grants permission to terminate Glue Studio Notebooks	Permissions management			
TestConnection	Grants permission to test connection in Glue Studio	Permissions management	connection		
			connectionType		
UntagResource	Grants permission to remove tags associated with a resource	Tagging	blueprint		
			catalog		
			connection		
			connectionType		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			crawler		
			customEntityType		
			dataQualityRuleset		
			database		
			devendpoint		
			integration		
			integrationResourceProperty		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workflow		
				aws:TagKeys glue:LakeFormationPermissions	
UpdateBlueprint	Grants permission to update a blueprint	Write	blueprint*		
UpdateCatalog	Grants permission to update a catalog	Write	rootcatalog*		
			catalog		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
UpdateClassifier	Grants permission to update a classifier	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateColumnStatisticsForPartition	Grants permission to update partition statistics of columns	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
UpdateColumnStatisticsForTable	Grants permission to update table statistics of columns	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	
UpdateColumnStatisticsTaskSettings	Grants permission to update settings for a column statistics task	Write	database*		
			rootcatalog*		
			table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnection	Grants permission to update a connection	Write	connection*		
			rootcatalog*		
			connectionType		
				glue:LakeFormationPermissions	
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
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
UpdateDevEndpoint	Grants permission to update a development endpoint	Write	devendpoint*		
UpdateGlueIdentityCenterConfiguration	Grants permission to update the managed Idc application	Write			
UpdateIntegrationResourceProperty	Grants permission to update the integration resource property	Write	catalog*		
			connection*		
			database*		
			integrationResourcePropertyarn*		
UpdateIntegrationTableProperties	Grants permission to update the integration table properties	Write	catalog*		
			connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
UpdatePartition	Grants permission to update a partition	Write	database*		
			rootcatalog*		
			table*		
			catalog		
				glue:LakeFormationPermissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				glue:LakeFormationPermissions glue:FederatedAuthorizationSource	
UpdateTableOptimizer	Grants permission to update the configuration for an existing table optimizer	Write	database*		glue:GetTable

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			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		
				glue:LakeFormationPermissions	
UpdateWorkflow	Grants permission to update a workflow	Write	workflow*		
UpgradeJob	Grants permission to upgrade a job to the latest version	Write	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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/${CatalogName}`	aws:ResourceTag/${TagKey}
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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}
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}

Resource types	ARN	Condition keys
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/${TagKey}
customEntityType	arn:${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/${TagKey}
connectionType	arn:${Partition}:glue:${Region}:${Account}:connectionType:${ConnectionTypeName}	aws:ResourceTag/${TagKey}
integrationResourceProperty	arn:${Partition}:glue:${Region}:${Account}:integrationresourceproperty/${ResourceType}/${ResourceName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Glue

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
glue:CredentialIssuingService	Filters access by the service from which the credentials of the request is issued	String
glue:EnabledForRedshiftAutoDiscovery	Filters access by the presence of the key configured for role's identity-based policy	Bool
glue:FederatedAuthorizationSource	Filters access by whether the resource belongs to federated authorization	String
glue:LakeFormationPermissions	Filters access by whether Lake Formation permission checks will be performed for a given caller and the Glue resource	String

Condition keys	Description	Type
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 AWS Glue DataBrew

AWS 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 AWS Glue DataBrew
- Resource types defined by AWS Glue DataBrew
- Condition keys for AWS Glue DataBrew

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteRecipeVersion	Grants permission to delete one or more recipe versions	Write	Recipe*		
CreateDataset	Grants permission to create a dataset	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProfileJob	Grants permission to create a profile job	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateProject	Grants permission to create a project	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecipe	Grants permission to create a recipe	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRecipeJob	Grants permission to create a recipe job	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRuleset	Grants permission to create a ruleset	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSchedule	Grants permission to create a schedule	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteDataset	Grants permission to delete a dataset	Write	Dataset*		
DeleteJob	Grants permission to delete a job	Write	Job*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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 AWS 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}
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 AWS Glue DataBrew

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Ground Station

AWS Ground Station (service prefix: `groundstation`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Ground Station
- Resource types defined by AWS Ground Station
- Condition keys for AWS Ground Station

Actions defined by AWS Ground Station

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelContact	Grants permission to cancel a contact	Write	Contact*		
CreateConfig	Grants permission to create a configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroup	Grants permission to create a data flow endpoint group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataflowEndpointGroupV2	Grants permission to create a data flow endpoint group using the V2 operation	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEphemeris	Grants permission to create an ephemeris item	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateMissionProfile	Grants permission to create a mission profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConfig	Grants permission to delete a config	Write	Config*		
DeleteDataflowEndpointGroup	Grants permission to delete a data flow endpoint group	Write	DataflowEndpointGroup*		
DeleteEphemeris	Grants permission to delete an ephemeris item	Write	EphemerisItem*		
DeleteMissionProfile	Grants permission to delete a mission profile	Write	MissionProfile*		
DescribeContact	Grants permission to describe a contact	Read	Contact*		
DescribeEphemeris	Grants permission to describe an ephemeris item	Read	EphemerisItem*		
GetAgentConfiguration	Grants permission to get the configuration of an agent	Read	Agent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAgentTaskResponseUrl	Grants permission to retrieve presigned S3 logging URLs	Read	Agent*		
GetConfig	Grants permission to return a configuration	Read	Config*		
GetDataflowEndpointGroup	Grants permission to return a data flow endpoint group	Read	DataflowEndpointGroup*		
GetMinuteUsage	Grants permission to return minutes usage	Read			
GetMissionProfile	Grants permission to retrieve a mission profile	Read	MissionProfile*		
GetSatellite	Grants permission to return information about a satellite	Read	Satellite*		
ListConfigs	Grants permission to return a list of past configurations	List			
ListContacts	Grants permission to return a list of contacts	List			
ListDataflowEndpointGroups	Grants permission to list data flow endpoint groups	List			
ListEphemerides	Grants permission to list ephemerides	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGroundStations	Grants permission to list ground stations	List			
ListMissionProfiles	Grants permission to return a list of mission profiles	List			
ListSatellites	Grants permission to list satellites	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	Config		
			Contact		
			DataflowEndpointGroup		
			MissionProfile		
RegisterAgent	Grants permission to register an agent	Write			
ReserveContact	Grants permission to reserve a contact	Write		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to assign a resource tag	Tagging	Config		
			Contact		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to unassign a resource tag	Tagging	Config		
			Contact		
			DataflowEndpointGroup		
			EphemerisItem		
			MissionProfile		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAgentStatus	Grants permission to update the status of an agent	Write	Agent*		
UpdateConfig	Grants permission to update a configuration	Write	Config*		
UpdateEphemeris	Grants permission to update an ephemeris item	Write	EphemerisItem*		
UpdateMissionProfile	Grants permission to update a mission profile	Write	MissionProfile*		

Resource types defined by AWS Ground Station

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
Config	`arn:${Partition}:groundstation:${Region}:${Account}:config/${ConfigType}/${ConfigId}`	aws:ResourceTag/${TagKey} groundstation:ConfigId groundstation:ConfigType

Resource types	ARN	Condition keys
Contact	arn:${Partition}:groundstation:${Region}:${Account}:contact/${ContactId}	aws:ResourceTag/${TagKey} groundstation:ContactId
DataflowEndpointGroup	arn:${Partition}:groundstation:${Region}:${Account}:dataflow-endpoint-group/${DataflowEndpointGroupId}	aws:ResourceTag/${TagKey} groundstation:DataflowEndpointGroupId
EphemerisItem	arn:${Partition}:groundstation:${Region}:${Account}:ephemeris/${EphemerisId}	aws:ResourceTag/${TagKey} groundstation:EphemerisId
GroundStationResource	arn:${Partition}:groundstation:${Region}:${Account}:groundstation:${GroundStationId}	groundstation:GroundStationId
MissionProfile	arn:${Partition}:groundstation:${Region}:${Account}:mission-profile/${MissionProfileId}	aws:ResourceTag/${TagKey} groundstation:MissionProfileId
Satellite	arn:${Partition}:groundstation:${Region}:${Account}:satellite/${SatelliteId}	groundstation:SatelliteId
Agent	arn:${Partition}:groundstation:${Region}:${Account}:agent/${AgentId}	groundstation:AgentId

Condition keys for AWS Ground Station

AWS Ground Station defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
groundstation:AgentId	Filters access by the ID of an agent	String
groundstation:ConfigId	Filters access by the ID of a config	String
groundstation:ConfigType	Filters access by the type of a config	String
groundstation:ContactId	Filters access by the ID of a contact	String
groundstation:DataflowEndpointGroupId	Filters access by the ID of a dataflow endpoint group	String

Condition keys	Description	Type
groundstation:EphemerisId	Filters access by the ID of an ephemeris	String
groundstation:GroundStationId	Filters access by the ID of a ground station	String
groundstation:MissionProfileId	Filters access by the ID of a mission profile	String
groundstation:SatelliteId	Filters access by the ID of a satellite	String

Actions, resources, and condition keys for Amazon GroundTruth Labeling

Amazon GroundTruth Labeling (service prefix: `groundtruthlabeling`) 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 GroundTruth Labeling
- Resource types defined by Amazon GroundTruth Labeling
- Condition keys for Amazon GroundTruth Labeling

Actions defined by Amazon GroundTruth Labeling

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociatePatchToManifestJob [permission only]	Grants permission to associate a patch file with the manifest file to update the manifest file	Write			
CreateBatch [permission only]	Grants permission to create a GT+ Batch	Write			
CreateIntakeForm [permission only]	Grants permission to create intake form	Write			
CreateProject [permission only]	Grants permission to create a GT+ Project	Write			
CreateWorkflowDefinition [permission only]	Grants permission to create a GT+ Workflow Definition	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConsoleJob [permission only]	Grants permission to get status of GroundTruthLabeling Jobs	Read			
GenerateLIDARPreviewTaskConfigJob [permission only]	Grants permission to generate LiDAR Preview Task	Write			
GetBatch [permission only]	Grants permission to get a GT + Batch	Read			
GetIntakeFormStatus [permission only]	Grants permission to get a intake forms	Read			
ListBatches [permission only]	Grants permission to list a GT + Batchs	Read			
ListDatasetObjects [permission only]	Grants permission to list dataset objects in a manifest file	Read			
ListProjects [permission only]	Grants permission to list a GT + Projects	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RunFilterOrSampleDatasetJob [permission only]	Grants permission to filter records from a manifest file using S3 select. Get sample entries based on random sampling	Write			
RunGenerateManifestByCrawlingJob [permission only]	Grants permission to list a S3 prefix and create manifest files from objects in that location	Write			
RunGenerateManifestMetricsJob [permission only]	Grants permission to generate metrics from objects in manifest	Write			
UpdateBatch [permission only]	Grants permission to update a GT+ Batch	Write			

Resource types defined by Amazon GroundTruth Labeling

Amazon GroundTruth Labeling does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon GroundTruth Labeling, specify `"Resource": "*"` in your policy.

Condition keys for Amazon GroundTruth Labeling

GroundTruth Labeling has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAdministratorInvitation	Grants permission to accept invitations to become a GuardDuty member account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIPSet	Grants permission to create an IPSet	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePublishingDestination	Grants permission to create a publishing destination	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateSampleFindings	Grants permission to create sample findings	Write			
CreateThreatEntitySet	Grants permission to create GuardDuty ThreatEntitySets, where a ThreatEntitySet consists of known malicious IP addresses and/or domains used by GuardDuty to generate findings	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateThreatIntelSet	Grants permission to create GuardDuty ThreatIntelSets, where a ThreatIntelSet consists of known malicious IP addresses used by GuardDuty to generate findings	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrustedEntitySet	Grants permission to create a TrustedEntitySet	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMembers	Grants permission to delete GuardDuty member accounts	Write			
DeletePublishingDestination	Grants permission to delete a publishing destination	Write	publishingDestination*		
DeleteThreatEntitySet	Grants permission to delete GuardDuty ThreatEntitySets	Write	threatentityset*		
DeleteThreatIntelSet	Grants permission to delete GuardDuty ThreatIntelSets	Write	threatintelset*		
DeleteTrustedEntitySet	Grants permission to delete GuardDuty TrustedEntitySets	Write	trustedentityset*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		
GetMalwareScan	Grants permission to retrieve a malware scan's details	Read			
GetMalwareScanSettings	Grants permission to retrieve the malware scan settings	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			
GetThreatEntitySet	Grants permission to retrieve GuardDuty ThreatEntitySets	Read	threatentityset*		
GetThreatIntelSet	Grants permission to retrieve GuardDuty ThreatIntelSets	Read	threatintelset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrustedEntitySet	Grants permission to retrieve GuardDuty TrustedEntitySets	Read	trustedentityset*		
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 AWS 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*		
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 AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMalwareProtectionPlans	Grants permission to retrieve a list of Malware Protection plans	List			
ListMalwareScans	Grants permission to retrieve a list of malware scans	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			
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		
			publishingDestination		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			threatentityset		
			threatintelset		
			trustedentityset		
ListThreatEntitySets	Grants permission to retrieve a list of GuardDuty ThreatEntitySets	List			
ListThreatIntelSets	Grants permission to retrieve a list of GuardDuty ThreatIntelSets	List			
ListTrustedEntitySets	Grants permission to retrieve a list of GuardDuty TrustedEntitySets	List			
SendObjectMalwareScan	Grants permission to initiate a new object malware scan	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMonitoringMembers	Grants permission to a GuardDuty administrator account to monitor findings from GuardDuty member accounts	Write			
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		
			publishingDestination		
			threatentityset		
			threatintelset		
			trustedentityset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
Unarchive Findings	Grants permission to unarchive GuardDuty findings	Write			
UntagResource	Grants permission to remove tags from a GuardDuty resource	Tagging	detector		
			filter		
			ipset		
			malwareprotectionplan		
			publishingDestination		
			threatentityset		
			threatintelset		
			trustedentityset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
UpdateThreatEntitySet	Grants permission to update GuardDuty ThreatEntitySets	Write	threatentityset*		s3:GetObject
UpdateThreatIntelSet	Grants permission to updates the GuardDuty ThreatIntelSets	Write	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateTrustedEntitySet	Grants permission to update GuardDuty TrustedEntitySets	Write	trustedentityset*		s3:GetObject

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/${TagKey}
trustedentityset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/trustedentityset/${TrustedEntitySetId}	aws:ResourceTag/${TagKey}
threatentityset	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatentityset/${ThreatEntitySetId}	aws:ResourceTag/${TagKey}
publishingDestination	arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingdestination/${PublishingDestinationId}	aws:ResourceTag/${TagKey}
malwareprotectionplan	arn:${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 AWS 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 AWS Health APIs and Notifications

AWS Health APIs and Notifications (service prefix: `health`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Health APIs and Notifications
- Resource types defined by AWS Health APIs and Notifications
- Condition keys for AWS Health APIs and Notifications

Actions defined by AWS Health APIs and Notifications

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAffectedAccountsForOrganization	Grants permission to retrieve a list of accounts that have been affected by the specified events in organization	Read			organizations:ListAccounts
DescribeAffectedEntities	Grants permission to retrieve a list of entities that have been affected by the specified events	Read	event*		
				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			
DescribeEntityAggr	Grants permission to retrieve the number of entities that are affected by each of	Read			organizations:ListAccounts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
egatesForOrganization	the specified events in an organization				
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 AWS Health APIs and Notifications

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

Condition keys for AWS Health APIs and Notifications

AWS Health APIs and Notifications defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
health:eventTypeCode	Filters access by event type	String
health:service	Filters access by impacted service	String

Actions, resources, and condition keys for AWS HealthImaging

AWS HealthImaging (service prefix: `medical-imaging`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS HealthImaging

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyImageSet	Grants permission to copy an image set	Write	datastore*		
			imageset*		
CreateDatastore	Grants permission to create a data store to ingest imaging data	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDatastore	Grants permission to delete a data store	Write	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteImageSet	Grants permission to delete an image set	Write	datastore*		
			imageset*		
GetDICOMBulkdata	Grants permission to get dicom bulkdata in binary format	Read	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
GetDICOMImportJob	Grants permission to get an import job's properties	Read	datastore*		
GetDICOMInstance	Grants permission to get dicom instance in dcm format	Read	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDICOMInstanceFrames	Grants permission to get dicom instance frames in format requested by the customer	Read	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
GetDICOMInstanceMetadata	Grants permission to get dicom instance metadata in DICOM JSON format	Read	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDICOMSeriesMetadata	Grants permission to retrieve metadata for all DICOM instances belonging to a given DICOM series in DICOM JSON format	Read	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
GetDatastore	Grants permission to get data store properties	Read	datastore*		
GetImageFrame	Grants permission to get image frame properties	Read	datastore*		
			imageset*		
GetImageSet	Grants permission to get image set properties	Read	datastore*		
			imageset*		
GetImageSetMetadata	Grants permission to get image set metadata properties	Read	datastore*		
			imageset*		
ListDICOMImportJobs	Grants permission to list import jobs for a data store	List	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatastores	Grants permission to list data stores	List			
ListImageSetVersions	Grants permission to list versions of an image set	List	datastore*		
			imageset*		
ListTagsForResource	Grants permission to list tags for a medical imaging resource	List	datastore		
			imageset		
SearchDICOMInstances	Grants permission to search dicom instances that returns data in DICOM JSON format	Read	datastore*		
				medical-imaging:StudyInstanceUID medical-imaging:SeriesInstanceUID	
SearchDICOMSeries	Grants permission to search dicom series that returns data in DICOM JSON format	Read	datastore*		
				medical-imaging:StudyInstanceUID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchDICOMStudies	Grants permission to search dicom studies that returns data in DICOM JSON format	Read	datastore*		
SearchImageSets	Grants permission to search image sets	Read	datastore*		
StartDICOMImportJob	Grants permission to start a DICOM import job	Write	datastore*		
StoreDICOM	Grants permission to store dicom instances that returns result in DICOM JSON format	Write	datastore*		
StoreDICOMStudy	Grants permission to store a dicom study that returns result in DICOM JSON format	Write	datastore*		
				medical-imaging:StudyInstanceUID	
TagResource	Grants permission to add tags to a medical imaging resource	Tagging	datastore		
			imageset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a medical imaging resource	Tagging	datastore		
			imageset		
				aws:TagKeys	
UpdateImageSetMetadata	Grants permission to update image set metadata properties	Write	datastore*		
			imageset*		

Resource types defined by AWS HealthImaging

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
datastore	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}`	aws:ResourceTag/${TagKey}
imageset	`arn:${Partition}:medical-imaging:${Region}:${Account}:datastore/${DatastoreId}/imageset/${ImageSetId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS HealthImaging

AWS HealthImaging defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
medical-imaging:SeriesInstanceUID	Filters access by the SeriesInstanceUID parameter in the request	String

Condition keys	Description	Type
medical-imaging:StudyInstanceUID	Filters access by the StudyInstanceUID parameter in the request	String

Actions, resources, and condition keys for AWS HealthLake

AWS HealthLake (service prefix: `healthlake`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS HealthLake
- Resource types defined by AWS HealthLake
- Condition keys for AWS HealthLake

Actions defined by AWS HealthLake

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelFHIRExportJobWithDelete	Grants permission to cancel an on going FHIR Export job with Delete	Write	datastore*		
ConfirmAttributionList	Grants permission to allow customers to indicate to a Producer that the Consumer does not have any more changes to be made to the Attribution List	Write	datastore*		
CreateFHIRDatastore	Grants permission to create a datastore that can ingest and export FHIR data	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateResource	Grants permission to create resource	Write	datastore*		
DeleteFHIRDatastore	Grants permission to delete a datastore	Write	datastore*		
DeleteResource	Grants permission to delete resource	Write	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFHIRBulkDeleteJob	Grants permission to describe a FHIR Bulk Delete Job	Read	datastore*		
DescribeFHIRDatastore	Grants permission to get the properties associated with the FHIR datastore, including the datastore ID, datastore ARN, datastore name, datastore status, created at, datastore type version, and datastore endpoint	Read	datastore*		
DescribeFHIRExportJob	Grants permission to display the properties of a FHIR export job, including the ID, ARN, name, and the status of the datastore	Read	datastore*		
DescribeFHIRExportJobWithGet	Grants permission to display the properties of a FHIR export job, including the ID, ARN, name, and the status of the datastore with Get	Read	datastore*		
DescribeFHIRImportJob	Grants permission to display the properties of a FHIR import job, including the ID, ARN, name, and the status of the datastore	Read	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExpandValueSetWithGet	Grants permission to search and expand ValueSet resource	Read	datastore*		
ExpandValueSetWithPost	Grants permission to search and expand ValueSet resource	Read	datastore*		
GenerateDocumentWithGet	Grants permission to generate a clinical document resource	Write	datastore*		
GenerateDocumentWithPost	Grants permission to generate a clinical document resource	Write	datastore*		
GetCapabilities	Grants permission to get the capabilities of a FHIR datastore	Read	datastore*		
GetExportedFile	Grants permission to access exported files from a FHIR Export job initiated with Get	Read	datastore*		
GetHistoryByResourceId	Grants permission to read resource history	Read	datastore*		
InquirePreAuthClaim	Grants permission to inquire about the status of a prior authorization Claim	Read	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFHIRDatastores	Grants permission to list all FHIR datastores that are in the user's account, regardless of datastore status	List			
ListFHIRExportJobs	Grants permission to get a list of export jobs for the specified datastore	List	datastore*		
ListFHIRImportJobs	Grants permission to get a list of import jobs for the specified datastore	List	datastore*		
ListTagsForResource	Grants permission to get a list of tags for the specified datastore	List	datastore		
LookupCodeSystemWithGet	Grants permission to retrieve Codes for a CodeSystem resource	Read	datastore*		
LookupCodeSystemWithPost	Grants permission to retrieve Codes for a CodeSystem resource	Read	datastore*		
MemberAdd	Grants permission to attribute a member with a specific provider group	Write	datastore*		
MemberMatch	Grants permission to enable cross-system patient matching	Write	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MemberRemove	Grants permission to remove a member from a group	Write	datastore*		
PatchResource	Grants permission to patch a resource	Write	datastore*		
ProcessBundle	Grants permission to bundle multiple resource operations	Write	datastore*		
QuestionnairePackage	Grants permission to retrieve Questionnaire packages with dependency Library and ValueSet resources	Read	datastore*		
ReadResource	Grants permission to read resource	Read	datastore*		
RetrieveAttributionStatus	Grants permission to retrieve member attribution status	Write	datastore*		
SearchEverything	Grants permission to search all resources related to a patient	Read	datastore*		
SearchWithGet	Grants permission to search resources with GET method	Read	datastore*		
SearchWithPost	Grants permission to search resources with POST method	Read	datastore*		
StartFHIRBulkDeleteJob	Grants permission to begin a FHIR Bulk Delete Job	Write	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartFHIRExportJob	Grants permission to begin a FHIR Export job	Write	datastore*		
StartFHIRExportJobWithGet	Grants permission to begin a FHIR Export job with Get	Write	datastore*		
StartFHIRExportJobWithPost	Grants permission to begin a FHIR Export job with Post	Write	datastore*		
StartFHIRImportJob	Grants permission to begin a FHIR Import job	Write	datastore*		
SubmitPreAuthClaim	Grants permission to submit a prior authorization Claim request	Write	datastore*		
TagResource	Grants permission to add tags to a datastore	Tagging	datastore		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove tags associated with a datastore	Tagging	datastore		
				aws:TagKeys	
UpdateResource	Grants permission to update resource	Write	datastore *		
ValidateResource	Grants permission to validate a resource	Read	datastore *		
VersionReadResource	Grants permission to read version of a resource	Read	datastore *		

Resource types defined by AWS HealthLake

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
datastore	`arn:${Partition}:healthlake:${Region}:${Account}:datastore/fhir/${DatastoreId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS HealthLake

AWS HealthLake defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 AWS HealthOmics

AWS HealthOmics (service prefix: `omics`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS HealthOmics
- Resource types defined by AWS HealthOmics
- Condition keys for AWS HealthOmics

Actions defined by AWS HealthOmics

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortMultipartReadSetUpload	Grants permission to abort multipart read set uploads	Write	sequenceStore*		
AcceptShare	Grants permission to accept a share	Write			
BatchDeleteReadSet	Grants permission to batch delete Read Sets in the given Sequence Store	Write	sequenceStore*		
CancelAnnotationImportJob	Grants permission to cancel an Annotation Import Job	Write			
CancelRun	Grants permission to cancel a workflow run and stop all workflow tasks	Write	run*		
CancelVariantImportJob	Grants permission to cancel a Variant Import Job	Write			
CompleteMultipartReadSetUpload	Grants permission to complete a multipart read set upload	Write	sequenceStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAnnotationStore	Grants permission to create an Annotation Store	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnnotationStoreVersion	Grants permission to create a Version in an Annotation Store	Write	AnnotationStore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Grants permission to create a new configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeSecurityGroups ec2:DescribeSubnets iam:CreateServiceLinkedRole
CreateMultipartReadSetUpload	Grants permission to create a multipart read set upload	Write	sequenceStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReferenceStore	Grants permission to create a Reference Store	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunCache	Grants permission to create a new workflow run cache	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRunGroup	Grants permission to create a new workflow run group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSequenceStore	Grants permission to create a Sequence Store	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateShare	Grants permission to create a share	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVariantStore	Grants permission to create a Variant Store	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflow	Grants permission to create a new workflow with a workflow definition and template of workflow parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowVersion	Grants permission to create a new workflow version with a workflow definition and template of workflow parameters	Write	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnnotationStore	Grants permission to delete an Annotation Store	Write	AnnotationStore*		
DeleteAnnotationStoreVersions	Grants permission to delete Versions in an Annotation Store	Write	AnnotationStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			AnnotationStoreVersion*		
DeleteConfiguration	Grants permission to delete a configuration	Write	configuration*		
DeleteReference	Grants permission to delete a Reference in the given Reference Store	Write	reference*		
			referenceStore*		
DeleteReferenceStore	Grants permission to delete a Reference Store	Write	referenceStore*		
DeleteRun	Grants permission to delete a workflow run	Write	run*		
DeleteRunCache	Grants permission to delete a workflow run cache	Write	runCache*		
DeleteRunGroup	Grants permission to delete a workflow run group	Write	runGroup*		
DeleteS3AccessPolicy	Grants permission to delete an access policy on a given store	Write	sequenceStore*		
DeleteSequenceStore	Grants permission to delete a Sequence Store	Write	sequenceStore*		
DeleteShare	Grants permission to delete a share	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVariantStore	Grants permission to delete a Variant Store	Write	VariantStore*		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow*		
DeleteWorkflowVersion	Grants permission to delete a workflow version	Write	WorkflowVersion*		
			workflow*		
GetAnnotationImportJob	Grants permission to get the status of an Annotation Import Job	Read			
GetAnnotationStore	Grants permission to get detailed information about an Annotation Store	Read	AnnotationStore*		
GetAnnotationStoreVersion	Grants permission to get detailed information about a version in an Annotation Store	Read	AnnotationStoreVersion*		
GetConfiguration	Grants permission to retrieve configuration details	Read	configuration*		
GetReadSet	Grants permission to get a Read Set in the given Sequence Store	Read	readSet*		
			sequenceStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReadSetActivationJob	Grants permission to get details about a Read Set activation job for the given Sequence Store	Read	sequenceStore*		
GetReadSetExportJob	Grants permission to get details about a Read Set export job for the given Sequence Store	Read	sequenceStore*		
GetReadSetImportJob	Grants permission to get details about a Read Set import job for the given Sequence Store	Read	sequenceStore*		
GetReadSetMetadata	Grants permission to get details about a Read Set in the given Sequence Store	Read	readSet*		
			sequenceStore*		
GetReference	Grants permission to get a Reference in the given Reference Store	Read	reference*		
			referenceStore*		
GetReferenceImportJob	Grants permission to get details about a Reference import job for the given Reference Store	Read	referenceStore*		
GetReferenceMetadata	Grants permission to get details about a Reference in the given Reference Store	Read	reference*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			referenceStore*		
GetReferenceStore	Grants permission to get details about a Reference Store	Read	referenceStore*		
GetRun	Grants permission to retrieve workflow run details	Read	run*		
GetRunCache	Grants permission to retrieve workflow run cache details	Read	runCache*		
GetRunGroup	Grants permission to retrieve workflow run group details	Read	runGroup*		
GetRunTask	Grants permission to retrieve workflow task details	Read	TaskResource*		
			run*		
GetS3AccessPolicy	Grants permission to get details about an access policy on a given store	Read	sequenceStore*		
GetSequenceStore	Grants permission to get details about a Sequence Store	Read	sequenceStore*		
GetShare	Grants permission to get detailed information about a Share	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVariantImportJob	Grants permission to get the status of a Variant Import Job	Read			
GetVariantStore	Grants permission to get detailed information about a Variant Store	Read	VariantStore*		
GetWorkflow	Grants permission to retrieve workflow details	Read	workflow*		
GetWorkflowVersion	Grants permission to retrieve workflow version details	Read	WorkflowVersion*		
			workflow*		
ListAnnotationImportJobs	Grants permission to get a list of Annotation Import Jobs	List			
ListAnnotationStoreVersions	Grants permission to retrieve a list of information about Versions in an Annotation Store	List	AnnotationStore*		
ListAnnotationStores	Grants permission to retrieve a list of information about Annotation Stores	List			
ListConfigurations	Grants permission to retrieve a list of configurations	List			
ListMultipartReadSetUploads	Grants permission to list multipart read set uploads	List	sequenceStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListReadSetActivationJobs	Grants permission to list Read Set activation jobs for the given Sequence Store	List	sequenceStore*		
ListReadSetExportJobs	Grants permission to list Read Set export jobs for the given Sequence Store	List	sequenceStore*		
ListReadSetImportJobs	Grants permission to list Read Set import jobs for the given Sequence Store	List	sequenceStore*		
ListReadSetUploadParts	Grants permission to list read set upload parts	List	sequenceStore*		
ListReadSets	Grants permission to list Read Sets in the given Sequence Store	List	sequenceStore*		
ListReferenceImportJobs	Grants permission to list Reference import jobs for the given Reference Store	List	referenceStore*		
ListReferenceStores	Grants permission to list Reference Stores	List			
ListReferences	Grants permission to list References in the given Reference Store	List	referenceStore*		
ListRunCaches	Grants permission to retrieve a list of workflow run caches	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRunGroups	Grants permission to retrieve a list of workflow run groups	List			
ListRunTasks	Grants permission to retrieve a list of tasks for a workflow run	List	run*		
ListRuns	Grants permission to retrieve a list of workflow runs	List			
ListSequenceStores	Grants permission to list Sequence Stores	List			
ListShares	Grants permission to retrieve a list of information about shares	List			
ListTagsForResource	Grants permission to retrieve a list of resource AWS tags	List			
ListVariantImportJobs	Grants permission to get a list of Variant Import Jobs	List			
ListVariantStores	Grants permission to retrieve a list of metadata for Variant Stores	List			
ListWorkflowVersions	Grants permission to retrieve a list of available versions for a workflow	List	workflow*		
ListWorkflows	Grants permission to retrieve a list of available workflows	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutS3AccessPolicy	Grants permission to put an access policy on a given store	Write	sequenceStore*		
StartAnnotationImportJob	Grants permission to import a list of Annotation files to an Annotation Store	Write	AnnotationStore*		
			AnnotationStoreVersion*		
StartReadSetActivationJob	Grants permission to start a Read Set activation job from the given Sequence Store	Write	sequenceStore*		
StartReadSetExportJob	Grants permission to start a Read Set export job from the given Sequence Store	Write	sequenceStore*		
StartReadSetImportJob	Grants permission to start a Read Set import job into the given Sequence Store	Write	sequenceStore*		
StartReferenceImportJob	Grants permission to start a Reference import job into the given Reference Store	Write	referenceStore*		
StartRun	Grants permission to start a workflow run	Write	run*		iam:PassRole
			configuration		
			runCache		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			runGroup		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartVariantImportJob	Grants permission to import a list of variant files to an Variant Store	Write	VariantStore*		
TagResource	Grants permission to add AWS tags to a resource	Tagging	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		
			WorkflowVersion		
			configuration		
			readSet		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove resource AWS tags	Tagging	AnnotationStore		
			AnnotationStoreVersion		
			VariantStore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			WorkflowVersion		
			configuration		
			readSet		
			reference		
			referenceStore		
			run		
			runCache		
			runGroup		
			sequenceStore		
			workflow		
				aws:TagKeys	
UpdateAnnotationStore	Grants permission to update information about the Annotation Store	Write	AnnotationStore*		
UpdateAnnotationStoreVersion	Grants permission to update information about the Version in an Annotation Store	Write	AnnotationStoreVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRunCache	Grants permission to update a workflow run cache	Write	runCache*		
UpdateRunGroup	Grants permission to update a workflow run group	Write	runGroup*		
UpdateSequenceStore	Grants permission to update details about a Sequence Store	Write	sequenceStore*		
UpdateVariantStore	Grants permission to update metadata about the Variant Store	Write	VariantStore*		
UpdateWorkflow	Grants permission to update workflow details	Write	workflow*		
UpdateWorkflowVersion	Grants permission to update workflow version details	Write	WorkflowVersion*		
			workflow*		
UploadReadSetPart	Grants permission to upload read set parts	Write	sequenceStore*		

Resource types defined by AWS HealthOmics

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
AnnotationStore	arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}	aws:ResourceTag/${TagKey}
AnnotationStoreVersion	arn:${Partition}:omics:${Region}:${Account}:annotationStore/${AnnotationStoreName}/version/${AnnotationStoreVersionName}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:omics:${Region}:${Account}:configuration/${Name}	aws:ResourceTag/${TagKey}
readSet	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}/readSet/${ReadSetId}	aws:ResourceTag/${TagKey}
reference	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}/reference/${ReferenceId}	aws:ResourceTag/${TagKey}
referenceStore	arn:${Partition}:omics:${Region}:${Account}:referenceStore/${ReferenceStoreId}	aws:ResourceTag/${TagKey}
run	arn:${Partition}:omics:${Region}:${Account}:run/${Id}	aws:ResourceTag/${TagKey}
runCache	arn:${Partition}:omics:${Region}:${Account}:runCache/${Id}	aws:ResourceTag/${TagKey}
runGroup	arn:${Partition}:omics:${Region}:${Account}:runGroup/${Id}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
sequenceStore	arn:${Partition}:omics:${Region}:${Account}:sequenceStore/${SequenceStoreId}	aws:ResourceTag/${TagKey}
TaskResource	arn:${Partition}:omics:${Region}:${Account}:task/${Id}	
VariantStore	arn:${Partition}:omics:${Region}:${Account}:variantStore/${VariantStoreName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}	aws:ResourceTag/${TagKey}
WorkflowVersion	arn:${Partition}:omics:${Region}:${Account}:workflow/${Id}/version/${VersionName}	aws:ResourceTag/${TagKey}

Condition keys for AWS HealthOmics

AWS HealthOmics defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by 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 Honeycode

Amazon Honeycode (service prefix: honeycode) 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 Honeycode
- Resource types defined by Amazon Honeycode
- Condition keys for Amazon Honeycode

Actions defined by Amazon Honeycode

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApproveTeamAssociation [permission only]	Grants permission to approve a team association request for your AWS Account	Write			
BatchCreateTableRows	Grants permission to create new rows in a table	Write	table*		
BatchDeleteTableRows	Grants permission to delete rows from a table	Write	table*		
BatchUpdateTableRows	Grants permission to update rows in a table	Write	table*		
BatchUpsertTableRows	Grants permission to upsert rows in a table	Write	table*		
CreateTeam [permission only]	Grants permission to create a new Amazon Honeycode team for your AWS Account	Write			
CreateTenant [permission only]	Grants permission to create a new tenant within Amazon Honeycode for your AWS Account	Write			
DeleteDomains [permission only]	Grants permission to delete Amazon Honeycode domains for your AWS Account	Write			
DeregisterGroups	Grants permission to remove groups from an Amazon	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]	Honeycode team for your AWS Account				
DescribeTableDataImportJob	Grants permission to get details about a table data import job	Read	table*		
DescribeTeam [permission only]	Grants permission to get details about Amazon Honeycode teams for your AWS Account	Read			
GetScreenData	Grants permission to load the data from a screen	Read	screen*		
InvokeScreenAutomation	Grants permission to invoke a screen automation	Write	screen-automation*		
ListDomains [permission only]	Grants permission to list all Amazon Honeycode domains and their verification status for your AWS Account	List			
ListGroups [permission only]	Grants permission to list all groups in an Amazon Honeycode team for your AWS Account	List			
ListTableColumns	Grants permission to list the columns in a table	List	table*		
ListTableRows	Grants permission to list the rows in a table	List	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTables	Grants permission to list the tables in a workbook	List	workbook*		
ListTagsForResource	Grants permission to list all tags for a resource	Tagging			
ListTeamAssociations [permission only]	Grants permission to list all pending and approved team associations with your AWS Account	List			
ListTenants [permission only]	Grants permission to list all tenants of Amazon Honeycode for your AWS Account	List			
QueryTableRows	Grants permission to query the rows of a table using a filter	Read	table*		
RegisterDomainForVerification [permission only]	Grants permission to request verification of the Amazon Honeycode domains for your AWS Account	Write			
RegisterGroups [permission only]	Grants permission to add groups to an Amazon Honeycode team for your AWS Account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectTeamAssociation [permission only]	Grants permission to reject a team association request for your AWS Account	Write			
RestartDomainVerification [permission only]	Grants permission to restart verification of the Amazon Honeycode domains for your AWS Account	Write			
StartTableDataImportJob	Grants permission to start a table data import job	Write	table*		
TagResource	Grants permission to tag a resource	Tagging			
UntagResource	Grants permission to untag a resource	Tagging			
UpdateTeam [permission only]	Grants permission to update an Amazon Honeycode team for your AWS Account	Write			

Resource types defined by Amazon Honeycode

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
workbook	arn:${Partition}:honeycode:${Region}:${Account}:workbook:workbook/${WorkbookId}	
table	arn:${Partition}:honeycode:${Region}:${Account}:table:workbook/${WorkbookId}/table/${TableId}	
screen	arn:${Partition}:honeycode:${Region}:${Account}:screen:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}	
screen-automation	arn:${Partition}:honeycode:${Region}:${Account}:screen-automation:workbook/${WorkbookId}/app/${AppId}/screen/${ScreenId}/automation/${AutomationId}	

Condition keys for Amazon Honeycode

Honeycode has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS IAM Access Analyzer

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessPreview	Grants permission to create an access preview for the specified analyzer	Write	Analyzer*		
CreateAnalyzer	Grants permission to create an analyzer	Write	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	Grants permission to create an archive rule for the specified analyzer	Write	ArchiveRule*		
DeleteAnalyzer	Grants permission to delete the specified analyzer	Write	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteArchiveRule	Grants permission to delete archive rules for the specified analyzer	Write	ArchiveRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFindingsStatistics	Grants permission to retrieve statistics for findings	Read	Analyzer*		
GetGeneratedPolicy	Grants permission to retrieve a policy that was generated using StartPolicyGeneration	Read			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidatePolicy	Grants permission to validate a policy	Read			

Resource types defined by AWS 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 AWS IAM Access Analyzer

AWS 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 AWS 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 AWS IAM Identity Center

AWS IAM Identity Center (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 AWS IAM Identity Center
- Resource types defined by AWS IAM Identity Center
- Condition keys for AWS IAM Identity Center

Actions defined by AWS IAM Identity Center

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddRegion	Grants permission to add a region to an IAM Identity Center instance	Write	Instance*		identitystore:AddRegion kms:Decrypt
Associate Directory	Grants permission to connect a directory to be used by AWS IAM Identity Center	Write			ds:AuthorizeApplication identitystore:CreateIdentityStore kms:Decrypt
Associate Profile	Grants permission to create an association between a directory user or group and a profile	Write			kms:Decrypt
AttachCustomerManagedPolicyReferenceToPermissionSet	Grants permission to attach a customer managed policy reference to a permission set	Permissions management	Instance* PermissionSet*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachManagedPolicyToPermissionSet	Grants permission to attach an AWS managed policy to a permission set	Permissions management	Instance*		kms:Decrypt
			PermissionSet*		
CreateAccountAssignment	Grants permission to assign access to a Principal for a specified AWS account using a specified permission set	Write	Account*		kms:Decrypt
			Instance*		
			PermissionSet*		
CreateApplication	Grants permission to create an application	Write	Application*		kms:Decrypt
			ApplicationProvider*		
			Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	Grants permission to create an application assignment	Write	Application*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
CreateApplicationInstance	Grants permission to add an application instance to AWS IAM Identity Center	Write			kms:Decrypt
CreateApplicationInstanceCertificate	Grants permission to add a new certificate for an application instance	Write			kms:Decrypt
CreateInstance	Grants permission to create an identity center instance	Write	Instance*		iam:CreateServiceLinkedRole identitystore:CreateIdentityStore 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 kms:Decrypt
CreateManagedApplicationInstance	Grants permission to add a managed application instance to AWS IAM Identity Center	Write			kms:Decrypt
CreatePermissionSet	Grants permission to create a permission set	Write	Instance*		kms:Decrypt
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Grants permission to create a profile for an application instance	Write			kms:Decrypt
CreateTrust	Grants permission to create a federation trust in a target account	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrustedTokenIssuer	Grants permission to create a trusted token issuer for an instance	Write	Instance*		kms:Decrypt
			TrustedTokenIssuer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	Grants permission to delete a Principal's access from a specified AWS account using a specified permission set	Write	Account*		kms:Decrypt
			Instance*		
			PermissionSet*		
DeleteApplication	Grants permission to delete an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationAccessScope	Grants permission to delete an access scope to an application	Write	Application*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
DeleteApplicationAssignment	Grants permission to delete an application assignment	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationAuthenticationMethod	Grants permission to delete an authentication method to an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationGrant	Grants permission to delete a grant from an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
DeleteApplicationInstance	Grants permission to delete the application instance	Write			kms:Decrypt
DeleteApplicationInstanceCertificate	Grants permission to delete an inactive or expired certificate from the application instance	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInlinePolicyFromPermissionSet	Grants permission to delete the inline policy from a specified permission set	Write	Instance*		kms:Decrypt
			PermissionSet*		
DeleteInstance	Grants permission to delete an identity center instance	Write	Instance*		identitystore:DeleteIdentityStore
DeleteInstanceAccessControlAttributeConfiguration	Grants permission to disable ABAC and remove the attributes list for the instance	Write	Instance*		kms:Decrypt
DeleteManagedApplicationInstance	Grants permission to delete the managed application instance	Write			kms:Decrypt
DeletePermissionSet	Grants permission to delete a permission set	Write	Instance*		kms:Decrypt
			PermissionSet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePermissionsBoundaryFromPermissionSet	Grants permission to remove permissions boundary from a permission set	Permissions management	Instance*		kms:Decrypt
			PermissionSet*		
DeleteProfile	Grants permission to delete the profile for an application instance	Write			kms:Decrypt
DeleteTrustedTokenIssuer	Grants permission to delete a trusted token issuer for an instance	Write	TrustedTokenIssuer*		kms:Decrypt
DescribeAccountAssignmentCreationStatus	Grants permission to describe the status of the assignment creation request	Read	Instance*		kms:Decrypt
DescribeAccountAssignmentDeletionStatus	Grants permission to describe the status of an assignment deletion request	Read	Instance*		kms:Decrypt
DescribeApplication	Grants permission to obtain information about an application	Read	Application*		kms:Decrypt
				sso:ApplicationAccount	
DescribeApplicationAssignment	Grants permission to retrieve an application assignment	Read	Application*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
DescribeApplicationProvider	Grants permission to describe an application provider	Read	ApplicationProvider*		
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*		kms:Decrypt
DescribePermissionSet	Grants permission to describe a permission set	Read	Instance*		kms:Decrypt
			PermissionSet*		
DescribePermissionSetProvisioningStatus	Grants permission to describe the status for the given Permission Set Provisioning request	Read	Instance*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRegion	Grants permission to retrieve configuration details for a specific IAM Identity Center instance region	Read	Instance*		kms:Decrypt
DescribeRegisteredRegions	Grants permission to obtain the regions where your organization has enabled AWS IAM Identity Center	Read			
DescribeTrustedTokenIssuer	Grants permission to describe a trusted token issuer for an instance	Read	TrustedTokenIssuer*		kms:Decrypt
DetachCustomerManagedPolicyReferenceFromPermissionSet	Grants permission to detach a customer managed policy reference from a permission set	Permissions management	Instance* PermissionSet*		kms:Decrypt
DetachManagedPolicyFromPermissionSet	Grants permission to detach the attached AWS managed policy from the specified permission set	Permissions management	Instance* PermissionSet*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateDirectory	Grants permission to disassociate a directory to be used by AWS IAM Identity Center	Write			ds:UnauthorizeApplication identitystore:DeleteIdentityStore kms:Decrypt
DisassociateProfile	Grants permission to disassociate a directory user or group from a profile	Write			kms:Decrypt
GetApplicationAccessScope	Grants permission to get an access scope to an application	Read	Application*		kms:Decrypt
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	Grants permission to read assignment configurations for an application	Read	Application*		kms:Decrypt
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	Grants permission to get an authentication method to an application	Read	Application*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
GetApplicationGrant	Grants permission to obtain details about a grant belonging to an application	Read	Application*		kms:Decrypt
				sso:ApplicationAccount	
GetApplicationInstance	Grants permission to retrieve details for an application instance	Read			kms:Decrypt
GetApplicationSessionConfiguration	Grants permission to get session configuration for an application	Read	Application*		kms:Decrypt
				sso:ApplicationAccount	
GetApplicationTemplate	Grants permission to retrieve application template details	Read			
GetInlinePolicyForPermissionSet	Grants permission to obtain the inline policy assigned to the permission set	Read	Instance*		kms:Decrypt
			PermissionSet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetManagedApplicationInstance	Grants permission to retrieve details for an application instance	Read			kms:Decrypt
GetMfaDeviceManagementForDirectory	Grants permission to retrieve Mfa Device Management settings for the directory	Read			kms:Decrypt
GetPermissionSet	Grants permission to retrieve details of a permission set	Read			kms:Decrypt
GetPermissionsBoundaryForPermissionSet	Grants permission to get permissions boundary for a permission set	Read	Instance*		kms:Decrypt
			PermissionSet*		
GetProfile	Grants permission to retrieve a profile for an application instance	Read			kms:Decrypt
GetSSOStatus	Grants permission to check if AWS IAM Identity Center is enabled	Read			
GetSharedSsoConfiguration	Grants permission to retrieve shared configuration for the current SSO instance	Read			kms:Decrypt
GetSsoConfiguration	Grants permission to retrieve configuration for the current SSO instance	Read			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrust	Grants permission to retrieve the federation trust in a target account	Read			kms:Decrypt
ImportApplicationInstanceServiceProviderMetadata	Grants permission to update the application instance by uploading an application SAML metadata file provided by the service provider	Write			kms:Decrypt
ListAccountAssignmentCreationStatus	Grants permission to list the status of the AWS account assignment creation requests for a specified SSO instance	List	Instance*		kms:Decrypt
ListAccountAssignmentDeletionStatus	Grants permission to list the status of the AWS account assignment deletion requests for a specified SSO instance	List	Instance*		kms:Decrypt
ListAccountAssignments	Grants permission to list the assignee of the specified AWS account with the specified permission set	List	Account*		kms:Decrypt
			Instance*		
			PermissionSet*		
ListAccountAssignmentsForPrincipal	Grants permission to list accounts assigned to user or group	List	Instance*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccountsForProvisionedPermissionSet	Grants permission to list all the AWS accounts where the specified permission set is provisioned	List	Instance*		kms:Decrypt
			PermissionSet*		
ListApplicationAccessScopes	Grants permission to list access scopes to an application	List	Application*		kms:Decrypt
				sso:ApplicationAccount	
ListApplicationAssignments	Grants permission to list application assignments	List	Application*		kms:Decrypt
				sso:ApplicationAccount	
ListApplicationAssignmentsForPrincipal	Grants permission to list applications assigned to user or group	List	Instance*		kms:Decrypt
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	Grants permission to list authentication methods to an application	List	Application*		kms:Decrypt
				sso:ApplicationAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplicationGrants	Grants permission to list grants from an application	List	Application*		kms:Decrypt
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	Grants permission to retrieve all of the certificates for a given application instance	Read			kms:Decrypt
ListApplicationInstances	Grants permission to retrieve all application instances	List			kms:Decrypt sso:GetApplicationInstance
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			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCustomerManagedPolicyReferencesInPermissionSet	Grants permission to list the customer managed policy references that are attached to a permission set	List	Instance* PermissionSet*		kms:Decrypt
ListDirectoryAssociations	Grants permission to retrieve details about the directory connected to AWS IAM Identity Center	Read			kms:Decrypt
ListInstances	Grants permission to list the SSO Instances that the caller has access to	List			
ListManagedPoliciesInPermissionSet	Grants permission to list the AWS managed policies that are attached to a specified permission set	List	Instance* PermissionSet*		kms:Decrypt
ListPermissionSetProvisioningStatus	Grants permission to list the status of the Permission Set Provisioning requests for a specified SSO instance	List	Instance*		kms:Decrypt
ListPermissionSets	Grants permission to retrieve all permission sets	List	Instance*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPermissionSetsProvisionedToAccount	Grants permission to list all the permission sets that are provisioned to a specified AWS account	List	Account*		kms:Decrypt
			Instance*		
ListProfileAssociations	Grants permission to retrieve the directory user or group associated with the profile	Read			kms:Decrypt
ListProfiles	Grants permission to retrieve all profiles for an application instance	List			kms:Decrypt sso:GetProfile
ListRegions	Grants permission to list all regions configured for an IAM Identity Center instance	List	Instance*		kms:Decrypt
ListTagsForResource	Grants permission to list the tags that are attached to a specified resource	Read	Application		kms:Decrypt
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
ListTrustedTokenIssuers	Grants permission to list trusted token issuers for an instance	List	Instance*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ProvisionPermissionSet	Grants permission to provision a specified permission set to the specified target	Write	Account*		kms:Decrypt
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	Grants permission to create/update an access scope to an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	Grants permission to add assignment configurations to an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	Grants permission to create/update an authentication method to an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
PutApplicationGrant	Grants permission to create/update a grant to an application	Write	Application*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
PutApplicationSessionConfiguration	Grants permission to put session configuration for an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
PutInlinePolicyToPermissionSet	Grants permission to attach an IAM inline policy to a permission set	Write	Instance*		kms:Decrypt
			PermissionSet*		
PutMfaDeviceManagementForDirectory	Grants permission to put Mfa Device Management settings for the directory	Write			kms:Decrypt
PutPermissionsBoundaryToPermissionSet	Grants permission to add permissions boundary to a permission set	Permissions management	Instance*		kms:Decrypt
			PermissionSet*		
PutPermissionsPolicy	Grants permission to add a policy to a permission set	Permissions management			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveRegion	Grants permission to remove a region from an IAM Identity Center instance	Write	Instance*		identitystore:RemoveRegion kms:Decrypt
SearchGroups	Grants permission to search for groups within the associated directory	Read			ds:DescribeDirectories kms:Decrypt
SearchUsers	Grants permission to search for users within the associated directory	Read			ds:DescribeDirectories kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSSO	Grants permission to initialize AWS IAM Identity Center	Write			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	Grants permission to associate a set of tags with a specified resource	Tagging	Application		kms:Decrypt
			Instance		
			PermissionSet		
			TrustedTokenIssuer		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to disassociate a set of tags from a specified resource	Tagging	Application		kms:Decrypt
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	Grants permission to update an application	Write	Application*		kms:Decrypt
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	Grants permission to set a certificate as the active one for this application instance	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplicationInstanceDisplayData	Grants permission to update display data of an application instance	Write			kms:Decrypt
UpdateApplicationInstanceResponseConfiguration	Grants permission to update federation response configuration for the application instance	Write			kms:Decrypt
UpdateApplicationInstanceResponseSchemaConfiguration	Grants permission to update federation response schema configuration for the application instance	Write			kms:Decrypt
UpdateApplicationInstanceSecurityConfiguration	Grants permission to update security details for the application instance	Write			kms:Decrypt
UpdateApplicationInstanceServiceProviderConfiguration	Grants permission to update service provider related configuration for the application instance	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplicationInstanceStatus	Grants permission to update the status of an application instance	Write			kms:Decrypt
UpdateInstance	Grants permission to update an identity center instance	Write	Instance*		identitystore:UpdateIdentityStore kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
UpdateInstanceAccessControlAttributeConfiguration	Grants permission to update the attributes to use with the instance for ABAC	Write	Instance*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateManagedApplicationInstanceStatus	Grants permission to update the status of a managed application instance	Write			kms:Decrypt
UpdatePermissionSet	Grants permission to update the permission set	Permissions management	Instance*		kms:Decrypt
			PermissionSet*		
UpdateProfile	Grants permission to update the profile for an application instance	Write			kms:Decrypt
UpdateSSOConfiguration	Grants permission to update the configuration for the current SSO instance	Write			kms:Decrypt
UpdateTrust	Grants permission to update the federation trust in a target account	Write			kms:Decrypt
UpdateTrustedTokenIssuer	Grants permission to update a trusted token issuer for an instance	Write	TrustedTokenIssuer*		kms:Decrypt

Resource types defined by AWS IAM Identity Center

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 AWS IAM Identity Center

AWS IAM Identity Center defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
identitycenter:ApplicationArn	Filters access by the ARN of the IAM Identity Center application	ARN
identitycenter:InstanceArn	Filters access by the ARN of the IAM Identity Center instance	ARN
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 AWS IAM Identity Center directory

AWS IAM Identity Center directory (service prefix: `sso-directory`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IAM Identity Center directory
- Resource types defined by AWS IAM Identity Center directory
- Condition keys for AWS IAM Identity Center directory

Actions defined by AWS IAM Identity Center directory

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddMemberToGroup	Grants permission to add a member to a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
CompleteVirtualMfaDeviceRegistration	Grants permission to complete the creation process of a virtual MFA device	Write			
CompleteWebAuthnDeviceRegistration	Grants permission to complete the registration process of a WebAuthn device	Write			
CreateAlias	Grants permission to create an alias for the directory that AWS IAM Identity Center provides by default	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBearerToken	Grants permission to create a bearer token for a given provisioning tenant	Write			kms:Decrypt
CreateExternalIdPConfigurationForDirectory	Grants permission to create an External Identity Provider configuration for the directory	Write			
CreateGroup	Grants permission to create a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
CreateProvisioningTenant	Grants permission to create a provisioning tenant for a given directory	Write			kms:Decrypt
CreateUser	Grants permission to create a user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
DeleteBearerToken	Grants permission to delete a bearer token	Write			kms:Decrypt
DeleteExternalIdPCertificate	Grants permission to delete the given external IdP certificate	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteExternalIdPConfigurationForDirectory	Grants permission to delete an External Identity Provider configuration associated with the directory	Write			
DeleteGroup	Grants permission to delete a group from the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
DeleteMfaDeviceForUser	Grants permission to delete a MFA device by device name for a given user	Write			
DeleteProvisioningTenant	Grants permission to delete the provisioning tenant	Write			kms:Decrypt
DeleteUser	Grants permission to delete a user from the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
DescribeDirectory	Grants permission to retrieve information about the directory that AWS IAM Identity Center provides by default	Read			
DescribeGroup	Grants permission to query the group data, not including user and group members	Read			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroups	Grants permission to retrieve information about groups from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
DescribeProvisioningTenant	Grants permission to describes the provisioning tenant	Read			kms:Decrypt
DescribeUser	Grants permission to retrieve information about a user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
DescribeUserByUniqueAttribute	Grants permission to describe user with a valid unique attribute represented for the user	Read			kms:Decrypt
DescribeUsers	Grants permission to retrieve information about user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
DisableExternalIdPConfigurationForDirectory	Grants permission to disable authentication of end users with an External Identity Provider	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableUser	Grants permission to deactivate a user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
EnableExternalIdPConfigurationForDirectory	Grants permission to enable authentication of end users with an External Identity Provider	Write			
EnableUser	Grants permission to activate user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
GetAWSSPConfigurationForDirectory	Grants permission to retrieve the AWS IAM Identity Center Service Provider configurations for the directory	Read			
GetGroupId	Grants permission to retrieve ID information about group from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
GetUserId	Grants permission to retrieve ID information about user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserPoolInfo	(Deprecated) Grants permission to get UserPool Info	Read			
ImportExternalIdPCertificate	Grants permission to import the IdP certificate used for verifying external IdP responses	Write			
IsMemberInGroup	Grants permission to check if a member is a part of the group in the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
IsMemberInGroups	Grants permission to check if a member is a part of multiple groups in the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListBearerTokens	Grants permission to list bearer tokens for a given provisioning tenant	Read			kms:Decrypt
ListExternalIdPCertificates	Grants permission to list the external IdP certificates of a given directory and IdP	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExternalIdPConfigurationsForDirectory	Grants permission to list all the External Identity Provider configurations created for the directory	Read			
ListGroups	Grants permission to list groups from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListGroupsForMember	Grants permission to list groups of the target member	Read			kms:Decrypt
ListGroupsForUser	Grants permission to list groups for a user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListMembersInGroup	Grants permission to retrieve all members that are part of a group in the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListMfaDevicesForUser	Grants permission to list all active MFA devices and their MFA device metadata for a user	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProvisioningTenants	Grants permission to list provisioning tenants for a given directory	Read			kms:Decrypt
ListUsers	Grants permission to list users from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
RemoveMemberFromGroup	Grants permission to remove a member that is part of a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
SearchGroups	Grants permission to search for groups within the associated directory	Read			kms:Decrypt
SearchUsers	Grants permission to search for users within the associated directory	Read			kms:Decrypt
StartVirtualMfaDeviceRegistration	Grants permission to begin the creation process of virtual mfa device	Write			
StartWebAuthnDeviceRegistration	Grants permission to begin the registration process of a WebAuthn device	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExternalIdPConfigurationForDirectory	Grants permission to update an External Identity Provider configuration associated with the directory	Write			
UpdateGroup	Grants permission to update information about a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
UpdateGroupDisplayName	Grants permission to update group display name update group display name response	Write			kms:Decrypt
UpdateMfaDeviceForUser	Grants permission to update MFA device information	Write			
UpdatePassword	Grants permission to update a password by sending password reset link via email or generating one time password for a user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUser	Grants permission to update user information in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
UpdateUserName	Grants permission to update user name update user name response	Write			kms:Decrypt
VerifyEmail	Grants permission to verify an email address of an User	Write			

Resource types defined by AWS IAM Identity Center directory

AWS IAM Identity Center directory does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS IAM Identity Center directory, specify `"Resource": "*"` in your policy.

Condition keys for AWS IAM Identity Center directory

IAM Identity Center directory has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS IAM Identity Center OIDC service

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTokenWithIAM	Grants permission to create and return OAuth 2.0 access tokens and refresh tokens for authorized client applications. These tokens might contain defined scopes that specify permissions such as `read:profile` or `write:data`	Write	Application*		kms:Decrypt
IntrospectTokenWithIAM [permission only]	Grants permission to validate and retrieve information about active OAuth 2.0 access tokens and refresh tokens, including their associated scopes and permissions. This permission is used only by AWS managed applications	Write	Application*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	and is not documented in the IAM Identity Center OIDC API Reference				
RevokeTokenWithIAM [permission only]	Grants permission to revoke OAuth 2.0 access tokens and refresh tokens, invalidating them before their normal expiration. This permission is used only by AWS managed applications and is not documented in the IAM Identity Center OIDC API Reference	Write	Application*		kms:Decrypt

Resource types defined by AWS 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 AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) (service prefix: `iam`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Identity and Access Management (IAM)
- Resource types defined by AWS Identity and Access Management (IAM)
- Condition keys for AWS Identity and Access Management (IAM)

Actions defined by AWS Identity and Access Management (IAM)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDelegationRequest	Accepts a delegation request resource, granting the requested temporary access	Write	delegation-request*		
AddClientIDToOpenIDConnectProvider	Grants permission to add a new client ID (audience) to the list of registered IDs for the specified IAM OpenID Connect (OIDC) provider resource	Write	oidc-provider*		
AddRoleToInstanceProfile	Grants permission to add an IAM role to the specified instance profile	Write	instance-profile*		iam:PassRole
AddUserToGroup	Grants permission to add an IAM user to the specified IAM group	Write	group*		
AssociateDelegationRequest	Associates a delegation request resource with the calling identity	Write	delegation-request*		
AttachGroupPolicy	Grants permission to attach a managed policy to the specified IAM group	Permissions management	group*		
				iam:PolicyARN	
AttachRolePolicy	Grants permission to attach a managed policy to the specified IAM role	Permissions management	role*		
				iam:PolicyARN	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:PermissionsBoundary	
AttachUserPolicy	Grants permission to attach a managed policy to the specified IAM user	Permissions management	user*		
				iam:PolicyARN iam:PermissionsBoundary	
ChangePassword	Grants permission to an IAM user to change their own password	Write	user*		
CreateAccessKey	Grants permission to create access key and secret access key for the specified IAM user	Write	user*		
CreateAccountAlias	Grants permission to create an alias for your AWS account	Write			
CreateDelegationRequest	Creates an IAM delegation request resource for temporary access delegation	Write	delegation-request*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:DelegationDuration iam:NotificationChannel iam:TemplateArn	
CreateGroup	Grants permission to create a new group	Write	group*		
CreateInstanceProfile	Grants permission to create a new instance profile	Write	instance-profile*		
				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 AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:ServiceSpecificCredentialAgeDays iam:ServiceSpecificCredentialServiceName	
CreateUser	Grants permission to create a new IAM user	Write	user*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	Grants permission to create a new virtual MFA device	Write	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeactivateMFADevice	Grants permission to deactivate the specified MFA device and remove its association with the IAM user for which it was originally enabled	Write	user*		
DeleteAccessKey	Grants permission to delete the access key pair that is associated with the specified IAM user	Write	user*		
DeleteAccountAlias	Grants permission to delete the specified AWS account alias	Write			
DeleteAccountPasswordPolicy	Grants permission to delete the password policy for the AWS account	Permissions management			
DeleteCloudFrontPublicKey	Grants permission to delete an existing CloudFront public key	Write			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInstanceProfile	Grants permission to delete the specified instance profile	Write	instance-profile*		
DeleteLoginProfile	Grants permission to delete the password for the specified IAM user	Write	user*		
DeleteOpenIDConnectProvider	Grants permission to delete an OpenID Connect identity provider (IdP) resource object in IAM	Write	oidc-provider*		
DeletePolicy	Grants permission to delete the specified managed policy and remove it from any IAM entities (users, groups, or roles) to which it is attached	Permissions management	policy*		
DeletePolicyVersion	Grants permission to delete a version from the specified managed policy	Permissions management	policy*		
DeleteRole	Grants permission to delete the specified role	Write	role*		
				iam:PermissionsBoundary	
DeleteRolePermissionsBoundary	Grants permission to remove the permissions boundary from a role	Permissions management	role*		
				iam:PermissionsBoundary	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRolePolicy	Grants permission to delete the specified inline policy from the specified role	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteSAMLProvider	Grants permission to delete a SAML provider resource in IAM	Write	saml-provider*		
DeleteSSHPublicKey	Grants permission to delete the specified SSH public key	Write	user*		
DeleteServerCertificate	Grants permission to delete the specified server certificate	Write	server-certificate*		
DeleteServiceLinkedRole	Grants permission to delete an IAM role that is linked to a specific AWS service, if the service is no longer using it	Write	role*		
DeleteServiceSpecificCredential	Grants permission to delete the specified service-specific credential for an IAM user	Write	user*		
				iam:ServiceSpecificCredentialServiceName	
DeleteSigningCertificate	Grants permission to delete a signing certificate that is associated with the specified IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUser	Grants permission to delete the specified IAM user	Write	user*		
DeleteUserPermissionsBoundary	Grants permission to remove the permissions boundary from the specified IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	Grants permission to delete the specified inline policy from an IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteVirtualMFADevice	Grants permission to delete a virtual MFA device	Write	mfa		
			sms-mfa		
DetachGroupPolicy	Grants permission to detach a managed policy from the specified IAM group	Permissions management	group*		
				iam:PolicyARN	
DetachRolePolicy	Grants permission to detach a managed policy from the specified role	Permissions management	role*		
				iam:PolicyARN	
				iam:PermissionsBoundary	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachUserPolicy	Grants permission to detach a managed policy from the specified IAM user	Permissions management	user*		
				iam:PolicyARN iam:PermissionsBoundary	
DisableOrganizationsRootCredentialsManagement	Grants permission to disable the management of member account root user credentials for an organization managed under the current account	Write			
DisableOrganizationsRootSessions	Grants permission to disable privileged root actions in member accounts for an organization managed under the current account	Write			
DisableOutboundWebIdentityFederation	Disables the outbound identity federation feature for the callers account	Write			
EnableMFADevice	Grants permission to enable an MFA device and associate it with the specified IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
EnableOrganizationsRootCredentialsManagement	Grants permission to enable the management of member account root user credentials for an organization managed under the current account	Write			
EnableOrganizationsRootSessions	Grants permission to enable privileged root actions in member accounts for an organization managed under the current account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOutboundWebIdentityFederation	Enables the outbound identity federation feature for the callers account	Write			
GenerateCredentialReport	Grants permission to generate a credential report for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateOrganizationsAccessReport	Grants permission to generate an access report for an AWS Organizations entity	Read	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy
				iam:OrganizationsPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateServiceLastAccessedDetails	Grants permission to generate a service last accessed data report for an IAM resource	Read	group*		
			policy*		
			role*		
			user*		
GetAccessKeyLastUsed	Grants permission to retrieve information about when the specified access key was last used	Read	user*		
GetAccountAuthorizationDetails	Grants permission to retrieve information about all IAM users, groups, roles, and policies in your AWS account, including their relationships to one another	Read			
GetAccountEmailAddress	Grants permission to retrieve the email address that is associated with the account	Read			
GetAccountName	Grants permission to retrieve the account name that is associated with the account	Read			
GetAccountPasswordPolicy	Grants permission to retrieve the password policy for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountSummary	Grants permission to retrieve information about IAM entity usage and IAM quotas in the AWS account	List			
GetCloudFrontPublicKey	Grants permission to retrieve information about the specified CloudFront public key	Read			
GetContextKeysForCustomPolicy	Grants permission to retrieve a list of all of the context keys that are referenced in the specified policy	Read			
GetContextKeysForPrincipalPolicy	Grants permission to retrieve a list of all context keys that are referenced in all IAM policies that are attached to the specified IAM identity (user, group, or role)	Read	group role user		
GetCredentialReport	Grants permission to retrieve a credential report for the AWS account	Read			
GetDelegationRequest	Retrieves information about a specific delegation request	Read	delegation-request*		
GetGroup	Grants permission to retrieve a list of IAM users in the specified IAM group	Read	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupPolicy	Grants permission to retrieve an inline policy document that is embedded in the specified IAM group	Read	group*		
GetHumanReadableSummary	Retrieves a human readable summary for a given entity. At this time, only delegation request are supported	Read	delegation-request*		
GetInstanceProfile	Grants permission to retrieve information about the specified instance profile, including the instance profile's path, GUID, ARN, and role	Read	instance-profile*		
GetLoginProfile	Grants permission to retrieve the user name and password creation date for the specified IAM user	List	user*		
GetMFADevice	Grants permission to retrieve information about an MFA device for the specified user	Read	user*		
GetOpenIDConnectProvider	Grants permission to retrieve information about the specified OpenID Connect (OIDC) provider resource in IAM	Read	oidc-provider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOrganizationsAccessReport	Grants permission to retrieve an AWS Organizations access report	Read			
GetOutboundWebIdentityFederationInfo	Retrieves the configuration information for the outbound identity federation feature for the callers account	Read			
GetPolicy	Grants permission to retrieve information about the specified managed policy, including the policy's default version and the total number of identities to which the policy is attached	Read	policy*		
GetPolicyVersion	Grants permission to retrieve information about a version of the specified managed policy, including the policy document	Read	policy*		
GetRole	Grants permission to retrieve information about the specified role, including the role's path, GUID, ARN, and the role's trust policy	Read	role*		
				iam:PermissionsBoundary	
GetRolePolicy	Grants permission to retrieve an inline policy document that is embedded with the specified IAM role	Read	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSAMLProvider	Grants permission to retrieve the SAML provider metadocument that was uploaded when the IAM SAML provider resource was created or updated	Read	saml-provider*		
GetSSHPublicKey	Grants permission to retrieve the specified SSH public key, including metadata about the key	Read	user*		
GetServerCertificate	Grants permission to retrieve information about the specified server certificate stored in IAM	Read	server-certificate*		
GetServiceLastAccessedDetails	Grants permission to retrieve information about the service last accessed data report	Read			
GetServiceLastAccessedDetailsWithEntities	Grants permission to retrieve information about the entities from the service last accessed data report	Read			
GetServiceLinkedRoleDeletionStatus	Grants permission to retrieve an IAM service-linked role deletion status	Read	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUser	Grants permission to retrieve information about the specified IAM user, including the user's creation date, path, unique ID, and ARN	Read	user*		
GetUserPolicy	Grants permission to retrieve an inline policy document that is embedded in the specified IAM user	Read	user*		
ListAccessKeys	Grants permission to list information about the access key IDs that are associated with the specified IAM user	List	user*		
ListAccountAliases	Grants permission to list the account alias that is associated with the AWS account	List			
ListAttachedGroupPolicies	Grants permission to list all managed policies that are attached to the specified IAM group	List	group*		
ListAttachedRolePolicies	Grants permission to list all managed policies that are attached to the specified IAM role	List	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAttachedUserPolicies	Grants permission to list all managed policies that are attached to the specified IAM user	List	user*		
ListCloudFrontPublicKeys	Grants permission to list all current CloudFront public keys for the account	List			
ListDelegationRequests	Lists delegation requests based on the specified criteria	List		iam:DelegationRequestOwner	
ListEntitiesForPolicy	Grants permission to list all IAM identities to which the specified managed policy is attached	List	policy*		
ListGroupPolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM group	List	group*		
ListGroups	Grants permission to list the IAM groups that have the specified path prefix	List			
ListGroupsForUser	Grants permission to list the IAM groups that the specified IAM user belongs to	List	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstanceProfileTags	Grants permission to list the tags that are attached to the specified instance profile	List	instance-profile*		
ListInstanceProfiles	Grants permission to list the instance profiles that have the specified path prefix	List			
ListInstanceProfilesForRole	Grants permission to list the instance profiles that have the specified associated IAM role	List	role*		
ListMFADeviceTags	Grants permission to list the tags that are attached to the specified virtual mfa device	List	mfa*		
ListMFADevices	Grants permission to list the MFA devices for an IAM user	List	user		
ListOpenIDConnectProviderTags	Grants permission to list the tags that are attached to the specified OpenID Connect provider	List	oidc-provider*		
ListOpenIDConnectProviders	Grants permission to list information about the IAM OpenID Connect (OIDC) provider resource objects that are defined in the AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOrganizationsFeatures	Grants permission to list the centralized root access features enabled for your organization	List			
ListPolicies	Grants permission to list all managed policies	List			
ListPoliciesGrantingServiceAccess	Grants permission to list information about the policies that grant an entity access to a specific service	List	group*		
			role*		
			user*		
ListPolicyTags	Grants permission to list the tags that are attached to the specified managed policy	List	policy*		
ListPolicyVersions	Grants permission to list information about the versions of the specified managed policy, including the version that is currently set as the policy's default version	List	policy*		
ListRolePolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM role	List	role*		
ListRoleTags	Grants permission to list the tags that are attached to the specified IAM role	List	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRoles	Grants permission to list the IAM roles that have the specified path prefix	List			
ListSAMLProviderTags	Grants permission to list the tags that are attached to the specified SAML provider	List	saml-provider*		
ListSAMLProviders	Grants permission to list the SAML provider resources in IAM	List			
ListSSHPublicKeys	Grants permission to list information about the SSH public keys that are associated with the specified IAM user	List	user*		
ListSTSRegionalEndpointsStatus	Grants permission to list the status of all active STS regional endpoints	List			
ListServerCertificateTags	Grants permission to list the tags that are attached to the specified server certificate	List	server-certificate*		
ListServerCertificates	Grants permission to list the server certificates that have the specified path prefix	List			
ListServiceSpecificCredentials	Grants permission to list the service-specific credentials that are associated with the specified IAM user	List	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSigningCertificates	Grants permission to list information about the signing certificates that are associated with the specified IAM user	List	user*		
ListUserPolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM user	List	user*		
ListUserTags	Grants permission to list the tags that are attached to the specified IAM user	List	user*		
ListUsers	Grants permission to list the IAM users that have the specified path prefix	List			
ListVirtualMFADevices	Grants permission to list virtual MFA devices by assignment status	List			
PassRole [permission only]	Grants permission to pass a role to a service	Write	role*		
				iam:AssociatedResourceArn iam:PassedToService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutGroupPolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM group	Permissions management	group*		
PutRolePermissionsBoundary	Grants permission to set a managed policy as a permissions boundary for a role	Permissions management	role*		
				iam:PermissionsBoundary	
PutRolePolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM role	Permissions management	role*		
				iam:PermissionsBoundary	
PutUserPermissionsBoundary	Grants permission to set a managed policy as a permissions boundary for an IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
PutUserPolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
RejectDelegationRequest	Rejects a delegation request, denying the requested temporary access	Write	delegation-request*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveClientIDFromOpenIDConnectProvider	Grants permission to remove the client ID (audience) from the list of client IDs in the specified IAM OpenID Connect (OIDC) provider resource	Write	oidc-provider*		
RemoveRoleFromInstanceProfile	Grants permission to remove an IAM role from the specified EC2 instance profile	Write	instance-profile*		
RemoveUserFromGroup	Grants permission to remove an IAM user from the specified group	Write	group*		
ResetServiceSpecificCredential	Grants permission to reset the password for an existing service-specific credential for an IAM user	Write	user*		
				iam:ServiceSpecificCredentialServiceName	
ResyncMFADevice	Grants permission to synchronize the specified MFA device with its IAM entity (user or role)	Write	user*		
SendDelegationToken	Sends the exchange token for an accepted delegation request	Write	delegation-request*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetDefaultPolicyVersion	Grants permission to set the version of the specified policy as the policy's default version	Permissions management	policy*		
SetSTSRegionalEndpointStatus	Grants permission to activate or deactivate an STS regional endpoint	Write			
SetSecurityTokenServicePreferences	Grants permission to set the STS global endpoint token version	Write			
SimulateCustomPolicy	Grants permission to simulate whether an identity-based policy or resource-based policy provides permissions for specific API operations and resources	Read			
SimulatePrincipalPolicy	Grants permission to simulate whether an identity-based policy that is attached to a specified IAM entity (user or role) provides permissions for specific API operations and resources	Read	group role user		
TagInstanceProfile	Grants permission to add tags to an instance profile	Tagging	instance-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	Grants permission to add tags to a virtual mfa device	Tagging	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	Grants permission to add tags to an OpenID Connect provider	Tagging	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	Grants permission to add tags to a managed policy	Tagging	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TagRole	Grants permission to add tags to an IAM role	Tagging	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagSAMLProvider	Grants permission to add tags to a SAML Provider	Tagging	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagServerCertificate	Grants permission to add tags to a server certificate	Tagging	server-certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	Grants permission to add tags to an IAM user	Tagging	user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	Grants permission to remove the specified tags from the instance profile	Tagging	instance-profile*		
				aws:TagKeys	
UntagMFADevice	Grants permission to remove the specified tags from the virtual mfa device	Tagging	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	Grants permission to remove the specified tags from the OpenID Connect provider	Tagging	oidc-provider*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagPolicy	Grants permission to remove the specified tags from the managed policy	Tagging	policy*		
				aws:TagKeys	
UntagRole	Grants permission to remove the specified tags from the role	Tagging	role*		
				aws:TagKeys	
UntagSAMLProvider	Grants permission to remove the specified tags from the SAML Provider	Tagging	saml-provider*		
				aws:TagKeys	
UntagServerCertificate	Grants permission to remove the specified tags from the server certificate	Tagging	server-certificate*		
				aws:TagKeys	
UntagUser	Grants permission to remove the specified tags from the user	Tagging	user*		
				aws:TagKeys	
UpdateAccessKey	Grants permission to update the status of the specified access key as Active or Inactive	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountEmailAddress	Grants permission to update the email address that is associated with the account	Write			
UpdateAccountName	Grants permission to update the account name that is associated with the account	Write			
UpdateAccountPasswordPolicy	Grants permission to update the password policy settings for the AWS account	Write			
UpdateAssumeRolePolicy	Grants permission to update the policy that grants an IAM entity permission to assume a role	Permissions management	role*		
				iam:PermissionsBoundary	
UpdateCloudFrontPublicKey	Grants permission to update an existing CloudFront public key	Write			
UpdateGroup	Grants permission to update the name or path of the specified IAM group	Write	group*		
UpdateLoginProfile	Grants permission to change the password for the specified IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOpenIDConnectProviderThumbprint	Grants permission to update the entire list of server certificate thumbprints that are associated with an OpenID Connect (OIDC) provider resource	Write	oidc-provider*		
UpdateRole	Grants permission to update the description or maximum session duration setting of a role	Write	role*		
				iam:PermissionsBoundary	
UpdateRoleDescription	Grants permission to update only the description of a role	Write	role*		
				iam:PermissionsBoundary	
UpdateSAMLProvider	Grants permission to update the metadata document for an existing SAML provider resource	Write	saml-provider*		
UpdateSSHPublicKey	Grants permission to update the status of an IAM user's SSH public key to active or inactive	Write	user*		
UpdateServerCertificate	Grants permission to update the name or the path of the specified server certificate stored in IAM	Write	server-certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceSpecificCredential	Grants permission to update the status of a service-specific credential to active or inactive for an IAM user	Write	user*		
				iam:ServiceSpecificCredentialServiceName	
UpdateSigningCertificate	Grants permission to update the status of the specified user signing certificate to active or disabled	Write	user*		
UpdateUser	Grants permission to update the name or the path of the specified IAM user	Write	user*		
UploadCloudFrontPublicKey	Grants permission to upload a CloudFront public key	Write			
UploadSSHPublicKey	Grants permission to upload an SSH public key and associate it with the specified IAM user	Write	user*		
UploadServerCertificate	Grants permission to upload a server certificate entity for the AWS account	Write	server-certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	Grants permission to upload an X.509 signing certificate and associate it with the specified IAM user	Write	user*		

Resource types defined by AWS Identity and Access Management (IAM)

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
access-report	`arn:${Partition}:iam::${Account}:access-report/${EntityPath}`	
assumed-role	`arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}`	

Resource types	ARN	Condition keys
federated-user	arn:${Partition}:iam::${Account}:federated-user/${UserName}	
group	arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}	
instance-profile	arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}	aws:ResourceTag/${TagKey}
mfa	arn:${Partition}:iam::${Account}:mfa/${MfaTokenIdWithPath}	aws:ResourceTag/${TagKey}
oidc-provider	arn:${Partition}:iam::${Account}:oidc-provider/${OidcProviderName}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:iam::${Account}:policy/${PolicyNameWithPath}	aws:ResourceTag/${TagKey}
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
saml-provider	arn:${Partition}:iam::${Account}:saml-provider/${SamlProviderName}	aws:ResourceTag/${TagKey}
server-certificate	arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}	aws:ResourceTag/${TagKey}
sms-mfa	arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}	

Resource types	ARN	Condition keys
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
delegation-request	arn:${Partition}:iam::${Account}:delegation-request/${DelegationRequestId}	iam:DelegationRequestOwner

Condition keys for AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString
iam:AWSServiceName	Filters access by the AWS service to which this role is attached	String

Condition keys	Description	Type
iam:AssociatedResourceArn	Filters access by the resource that the role will be used on behalf of	ARN
iam:DelegationDuration	Filters access based on the requested delegation duration	String
iam:DelegationRequestOwner	Filters access based on the delegation request owner	ARN
iam:FIDO-FIPS-140-2-certification	Filters access by the MFA device FIPS-140-2 validation certification level at the time of registration of a FIDO security key	String
iam:FIDO-FIPS-140-3-certification	Filters access by the MFA device FIPS-140-3 validation certification level at the time of registration of a FIDO security key	String
iam:FIDO-certification	Filters access by the MFA device FIDO certification level at the time of registration of a FIDO security key	String
iam:NotificationChannel	Filters access based on the requested notification channel	String
iam:OrganizationsPolicyId	Filters access by the ID of an AWS Organizations policy	String
iam:PassedToService	Filters access by the AWS service to which this role is passed	String
iam:PermissionsBoundary	Filters access if the specified policy is set as the permissions boundary on the IAM entity (user or role)	ARN
iam:PolicyARN	Filters access by the ARN of an IAM policy	ARN

Condition keys	Description	Type
iam:RegisterSecurityKey	Filters access by the current state of MFA device enablement	String
iam:ResourceTag/${TagKey}	Filters access by the tags attached to an IAM entity (user or role)	String
iam:ServiceSpecificCredentialAgeDays	Filters access by the duration until the credential's expiration	Numeric
iam:ServiceSpecificCredentialServiceName	Filters access by the service associated with the credential	String
iam:TemplateArn	Filters access based on the requested template ARN	ARN

Actions, resources, and condition keys for AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere (service prefix: `rolesanywhere`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Identity and Access Management Roles Anywhere

- Resource types defined by AWS Identity and Access Management Roles Anywhere
- Condition keys for AWS Identity and Access Management Roles Anywhere

Actions defined by AWS Identity and Access Management Roles Anywhere

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProfile	Grants permission to create a profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	Grants permission to create a trust anchor	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAttributeMapping	Grants permission to delete a mapping rule from a profile	Write	profile*		
DeleteCrl	Grants permission to delete a certificate revocation list (crl)	Write	crl*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProfile	Grants permission to delete a profile	Write	profile*		
DeleteTrustAnchor	Grants permission to delete a trust anchor	Write	trust-anchor*		
DisableCrl	Grants permission to disable a certificate revocation list (crl)	Write	crl*		
DisableProfile	Grants permission to disable a profile	Write	profile*		
DisableTrustAnchor	Grants permission to disable a trust anchor	Write	trust-anchor*		
EnableCrl	Grants permission to enable a certificate revocation list (crl)	Write	crl*		
EnableProfile	Grants permission to enable a profile	Write	profile*		iam:PassRole
EnableTrustAnchor	Grants permission to enable a trust anchor	Write	trust-anchor*		
GetCrl	Grants permission to get a certificate revocation list (crl)	Read	crl*		
GetProfile	Grants permission to get a profile	Read	profile*		
GetSubject	Grants permission to get a subject	Read	subject*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrustAnchor	Grants permission to get a trust anchor	Read	trust-anchor*		
ImportCrl	Grants permission to import a certificate revocation list (crl)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	Grants permission to list certificate revocation lists (crls)	List			
ListProfiles	Grants permission to list profiles	List			
ListSubjects	Grants permission to list subjects	List			
ListTagsForResource	Grants permission to list tags for a resource	List			
ListTrustAnchors	Grants permission to list trust anchors	List			
PutAttributeMapping	Grants permission to put a mapping rule into a profile	Write	profile*		
PutNotificationSettings	Grants permission to attach notification settings to a trust anchor	Write	trust-anchor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetNotificationSettings	Grants permission to reset custom notification settings to IAM Roles Anywhere defined default state	Write	trust-anchor*		
TagResource	Grants permission to tag a resource	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCrl	Grants permission to update a certificate revocation list (crl)	Write	crl*		
UpdateProfile	Grants permission to update a profile	Write	profile*		iam:PassRole
UpdateTrustAnchor	Grants permission to update a trust anchor	Write	trust-anchor*		

Resource types defined by AWS Identity and Access Management Roles Anywhere

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
trust-anchor	`arn:${Partition}:rolesanywhere:${Region}:${Account}:trust-anchor/${TrustAnchorId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:rolesanywhere:${Region}:${Account}:profile/${ProfileId}`	aws:ResourceTag/${TagKey}
subject	`arn:${Partition}:rolesanywhere:${Region}:${Account}:subject/${SubjectId}`	aws:ResourceTag/${TagKey}
crl	`arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Identity Store

AWS Identity Store (service prefix: `identitystore`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Identity Store
- Resource types defined by AWS Identity Store
- Condition keys for AWS Identity Store

Actions defined by AWS Identity Store

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddRegion	Grants permission to add a region to an IdentityStore	Write			kms:Decrypt
CreateGroup	Grants permission to create a group in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
CreateGroupMembership	Grants permission to create a member to a group in the specified IdentityStore	Write	Group*		kms:Decrypt
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIdentityStore	Grants permission to create a new IdentityStore in an AWS account	Write			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
CreateUser	Grants permission to create a user in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers identitystore:ReservedUserId	
DeleteGroup	Grants permission to delete a group in the specified IdentityStore	Write	Group*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Identitystore*		
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
DeleteGroupMembership	Grants permission to remove a member that is part of a group in the specified IdentityStore	Write	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
DeleteIdentityStore	Grants permission to delete an IdentityStore	Write			
DeleteUser	Grants permission to delete a user in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
DescribeGroup	Grants permission to retrieve information about a group in the specified IdentityStore	Read	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
DescribeGroupMembership	Grants permission to retrieve information about a member that is part of a group in the specified IdentityStore	Read	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion	
DescribeRegion	Grants permission to retrieve configuration details for a specific IdentityStore region	Read		identitystore:PrimaryRegion	kms:Decrypt
DescribeUser	Grants permission to retrieve information about user in the specified IdentityStore	Read	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
GetGroupId	Grants permission to retrieve ID information about group in the specified IdentityStore	Read	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupMembershipId	Grants permission to retrieve ID information of a member which is part of a group in the specified IdentityStore	Read	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
GetUserId	Grants permission to retrieves ID information about user in the specified IdentityStore	Read	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion	
IsMemberInGroups	Grants permission to check if a member is a part of groups in the specified IdentityStore	Read	AllGroupMemberships*		kms:Decrypt
			Group*		
			Identitystore*		
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion	
ListGroupMemberships	Grants permission to retrieve all members that are part of a group in the specified IdentityStore	List	AllGroupMemberships*		kms:Decrypt
			Group*		
			Identitystore*		
				identitystore:PrimaryRegion	
ListGroupMembershipsForMember	Grants permission to list groups of the target member in the specified IdentityStore	List	AllGroupMemberships*		kms:Decrypt
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
ListGroups	Grants permission to search for groups within the specified IdentityStore	List	AllGroups*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Identitystore*		
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
ListRegions	Grants permission to list all regions configured for an IdentityStore	List		identitystore:PrimaryRegion	kms:Decrypt
ListUsers	Grants permission to search for users in the specified IdentityStore	List	AllUsers*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
RemoveRegion	Grants permission to remove a region from an IdentityStore	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReserveUser	Grants permission to reserve a user by getting a userId	Write	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion	
UpdateGroup	Grants permission to update information about a group in the specified IdentityStore	Write	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion	
				identitystore:GroupExternalIdIssuers	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIdentityStore	Grants permission to update the configuration of an IdentityStore	Write			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
UpdateUser	Grants permission to update user information in the specified IdentityStore	Write	Identitystore* User*	 identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	kms:Decrypt

Resource types defined by AWS Identity Store

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
Identitystore	`arn:${Partition}:identitystore::${Account}:identitystore/${IdentityStoreId}`	
User	`arn:${Partition}:identitystore:::user/${UserId}`	
Group	`arn:${Partition}:identitystore:::group/${GroupId}`	
GroupMembership	`arn:${Partition}:identitystore:::membership/${MembershipId}`	
AllUsers	`arn:${Partition}:identitystore:::user/*`	
AllGroups	`arn:${Partition}:identitystore:::group/*`	
AllGroupMemberships	`arn:${Partition}:identitystore:::membership/*`	

Condition keys for AWS Identity Store

AWS Identity Store defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
identitystore:GroupExternalIdIssuers	Filters access by Issuer present in ExternalIds for Group resources	ArrayOfARN
identitystore:IdentityStoreArn	Filters access by Identity Store ARN	ARN
identitystore:PrimaryRegion	Filters access by Primary Region of Identity Store	String
identitystore:ReservedUserId	Filters access by a previously reserved User ID for CreateUser operation	String
identitystore:UserExternalIdIssuers	Filters access by Issuer present in ExternalIds for User resources	ArrayOfARN
identitystore:UserId	Filters access by Identity Store User ID	String

Actions, resources, and condition keys for AWS Identity Store Auth

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Identity Store Auth

AWS Identity Store Auth does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Identity Store Auth, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Identity Sync

AWS 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 AWS Identity Sync
- Resource types defined by AWS Identity Sync
- Condition keys for AWS Identity Sync

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource	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 AWS 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 AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Import Export Disk Service

AWS Import Export Disk Service (service prefix: `importexport`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Import Export Disk Service
- Resource types defined by AWS Import Export Disk Service

- Condition keys for AWS Import Export Disk Service

Actions defined by AWS Import Export Disk Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelJob	This action cancels a specified job. Only the job owner can cancel it. The action fails if the job has already started or is complete.	Write			
CreateJob	This action initiates the process of scheduling an upload or download of your data.	Write			
GetShippingLabel	This action generates a pre-paid shipping label that you will use to ship your device to AWS for processing.	Read			
GetStatus	This action returns information about a job, including where the job is in the processing pipeline, the status of the results, and the	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	signature value associated with the job.				
ListJobs	This action returns the jobs associated with the requester.	List			
UpdateJob	You use this action to change the parameters specified in the original manifest file by supplying a new manifest file.	Write			

Resource types defined by AWS Import Export Disk Service

AWS Import Export Disk Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Import Export Disk Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Import Export Disk Service

Import/Export has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Inspector

Amazon Inspector (service prefix: `inspector`) 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 Inspector

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAttributesToFindings	Grants permission to assign attributes (key and value pairs) to the findings that are specified by the ARNs of the findings	Write			
CreateAssessmentTarget	Grants permission to create a new assessment target using the ARN of the resource group that is generated by CreateResourceGroup	Write			
CreateAssessmentTemplate	Grants permission to create an assessment template for the assessment target that is specified by the ARN of the assessment target	Write			
CreateExclusionsPreview	Grants permission to start the generation of an exclusions preview for the specified assessment template	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResourceGroup	Grants permission to create a resource group using the specified set of tags (key and value pairs) that are used to select the EC2 instances to be included in an Amazon Inspector assessment target	Write			
DeleteAssessmentRun	Grants permission to delete the assessment run that is specified by the ARN of the assessment run	Write			
DeleteAssessmentTarget	Grants permission to delete the assessment target that is specified by the ARN of the assessment target	Write			
DeleteAssessmentTemplate	Grants permission to delete the assessment template that is specified by the ARN of the assessment template	Write			
DescribeAssessmentRuns	Grants permission to describe the assessment runs that are specified by the ARNs of the assessment runs	Read			
DescribeAssessmentTargets	Grants permission to describe the assessment targets that are specified by the ARNs of the assessment targets	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAssessmentTemplates	Grants permission to describe the assessment templates that are specified by the ARNs of the assessment templates	Read			
DescribeCrossAccountAccessRole	Grants permission to describe the IAM role that enables Amazon Inspector to access your AWS account	Read			
DescribeExclusions	Grants permission to describe the exclusions that are specified by the exclusions' ARNs	Read			
DescribeFindings	Grants permission to describe the findings that are specified by the ARNs of the findings	Read			
DescribeResourceGroups	Grants permission to describe the resource groups that are specified by the ARNs of the resource groups	Read			
DescribeRulesPackages	Grants permission to describe the rules packages that are specified by the ARNs of the rules packages	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssessmentReport	Grants permission to produce an assessment report that includes detailed and comprehensive results of a specified assessment run	Read			
GetExclusionsPreview	Grants permission to retrieve the exclusions preview (a list of ExclusionPreview objects) specified by the preview token	Read			
GetTelemetryMetadata	Grants permission to get information about the data that is collected for the specified assessment run	Read			
ListAssessmentRunAgents	Grants permission to list the agents of the assessment runs that are specified by the ARNs of the assessment runs	List			
ListAssessmentRuns	Grants permission to list the assessment runs that correspond to the assessment templates that are specified by the ARNs of the assessment templates	List			
ListAssessmentTargets	Grants permission to list the ARNs of the assessment targets within this AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssessmentTemplates	Grants permission to list the assessment templates that correspond to the assessment targets that are specified by the ARNs of the assessment targets	List			
ListEventSubscriptions	Grants permission to list all the event subscriptions for the assessment template that is specified by the ARN of the assessment template	List			
ListExclusions	Grants permission to list exclusions that are generated by the assessment run	List			
ListFindings	Grants permission to list findings that are generated by the assessment runs that are specified by the ARNs of the assessment runs	List			
ListRulesPackages	Grants permission to list all available Amazon Inspector rules packages	List			
ListTagsForResource	Grants permission to list all tags associated with an assessment template	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PreviewAgents	Grants permission to preview the agents installed on the EC2 instances that are part of the specified assessment target	Read			
RegisterCrossAccountAccessRole	Grants permission to register the IAM role that Amazon Inspector uses to list your EC2 instances at the start of the assessment run or when you call the PreviewAgents action	Write			
RemoveAttributesFromFindings	Grants permission to remove entire attributes (key and value pairs) from the findings that are specified by the ARNs of the findings where an attribute with the specified key exists	Write			
SetTagsForResource	Grants permission to set tags (key and value pairs) to the assessment template that is specified by the ARN of the assessment template	Tagging			
StartAssessmentRun	Grants permission to start the assessment run specified by the ARN of the assessment template	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopAssessmentRun	Grants permission to stop the assessment run that is specified by the ARN of the assessment run	Write			
SubscribeToEvent	Grants permission to enable the process of sending Amazon Simple Notification Service (SNS) notifications about a specified event to a specified SNS topic	Write			
UnsubscribeFromEvent	Grants permission to disable the process of sending Amazon Simple Notification Service (SNS) notifications about a specified event to a specified SNS topic	Write			
UpdateAssessmentTarget	Grants permission to update the assessment target that is specified by the ARN of the assessment target	Write			

Resource types defined by Amazon Inspector

Amazon Inspector does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Inspector, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Inspector

Inspector has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Member	Grants permission to associate an account with an Amazon Inspector administrator account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAssociateCodeSecurityScanConfiguration	Grants permission to associate multiple code repositories with an Amazon Inspector code security scan configuration	Write			
BatchDisassociateCodeSecurityScanConfiguration	Grants permission to disassociate multiple code repositories from an Amazon Inspector code security scan configuration	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetMemberEc2DeepInspectionStatus	Grants permission to delegated administrator to retrieve ec2 deep inspection status of member accounts	Read			
BatchUpdateMemberEc2DeepInspectionStatus	Grants permission to update ec2 deep inspection status by delegated administrator for its associated member accounts	Write			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityIntegration	Grants permission to create a code security integration with a source code repository provider	Write	Code Security Integration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCodeSecurityScanConfiguration	Grants permission to create a scan configuration for code security scanning	Write	Code Security Scan Configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	Grants permission to create and define the settings for a findings filter	Write	Filter*		
				aws:RequestTag/${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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCodeSecurityIntegration	Grants permission to delete a code security integration	Write	CodeSecurityIntegration*		
DeleteCodeSecurityScanConfiguration	Grants permission to delete a code security scan configuration	Write	CodeSecurityScanConfiguration*		
DeleteFilter	Grants permission to delete a findings filter	Write	Filter*		
DescribeOrganizationConfiguration	Grants permission to retrieve information about the Amazon Inspector configuration settings for an AWS organization	Read			
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 AWS organization	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS organization	Write			
GetCisScanReport	Grants permission to retrieve a report containing information about completed CIS scans	Read			
GetCisScanResultDetails	Grants permission to retrieve information about all details pertaining to one CIS scan and one targeted resource	List			
GetClustersForImage	Grants permission to get cluster information for a given a continuously scanned amazon Ecr image	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCodeSecurityIntegration	Grants permission to retrieve information about a code security integration	Read			
GetCodeSecurityScan	Grants permission to retrieve information about a specific code security scan	Read			
GetCodeSecurityScanConfiguration	Grants permission to retrieve information about a code security scan configuration	Read			
GetConfiguration	Grants permission to retrieve information about the Amazon Inspector configuration settings for an AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListCodeSecurityIntegrations	Grants permission to list all code security integrations in your account	List			
ListCodeSecurityScanConfigurationAssociations	Grants permission to list the associations between code repositories and Amazon Inspector code security scan configurations	List			
ListCodeSecurityScanConfigurations	Grants permission to list all code security scan configurations in your account	List			
ListCoverage	Grants permission to retrieve the types of statistics Amazon Inspector can generate for resources Inspector monitors	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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			
ListMembers	Grants permission to retrieve information about the Amazon Inspector member accounts that are associated with an Inspector administrator account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
StartCisSession	Grants permission to start a CIS scan session	Write			
StartCodeSecurityScan	Grants permission to initiate a code security scan on a specified repository	Write			
StopCisSession	Grants permission to stop a CIS scan session	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add or update the tags for an Amazon Inspector resource	Tagging	CIS Scan Configuration		
			Code Security Integration		
			Code Security Scan Configuration		
			Filter		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from an Amazon Inspector resource	Tagging	CIS Scan Configuration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Code Security Integration		
			Code Security Scan Configuration		
			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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCodeSecurityIntegration	Grants permission to update an existing code security integration	Write	Code Security Integration*		
				aws:ResourceTag/${TagKey}	
UpdateCodeSecurityScanConfiguration	Grants permission to update an existing code security scan configuration	Write	Code Security Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	Grants permission to update information about the Amazon Inspector configuration settings for an AWS 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 AWS 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}
Code Security Scan Configuration	arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/codesecurity-configuration/${CodeSecurityScanConfigurationId}	aws:ResourceTag/${TagKey}
Code Security Integration	arn:${Partition}:inspector2:${Region}:${Account}:codesecurity-integration/${CodeSecurityIntegrationId}	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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Inspector2 Telemetry Channel

Amazon Inspector2 Telemetry Channel (service prefix: `inspector2-telemetry`) 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 Telemetry Channel
- Resource types defined by Amazon Inspector2 Telemetry Channel
- Condition keys for Amazon Inspector2 Telemetry Channel

Actions defined by Amazon Inspector2 Telemetry Channel

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyHeartbeat	Grants permission to notify heartbeat for an active telemetry session	Write			
SendTelemetry	Grants permission to send telemetry for an active telemetry session	Write			
StartSession	Grants permission to start a telemetry session	Write			
StopSession	Grants permission to stop a telemetry session	Write			

Resource types defined by Amazon Inspector2 Telemetry Channel

Amazon Inspector2 Telemetry Channel does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Inspector2 Telemetry Channel, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Inspector2 Telemetry Channel

Inspector2Telemtry has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon InspectorScan

Amazon InspectorScan (service prefix: `inspector-scan`) 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 InspectorScan

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ScanSbom	Grants permission to scan the customer provided SBOM and return vulnerabilities detected within	Read			

Resource types defined by Amazon InspectorScan

Amazon InspectorScan does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon InspectorScan, specify `"Resource": "*"` in your policy.

Condition keys for Amazon InspectorScan

InspectorScan has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Interactive Video Service

Amazon Interactive Video Service (service prefix: `ivs`) 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 Interactive Video Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetChannel	Grants permission to get multiple channels simultaneously by channel ARN	Read	Channel*		
BatchGetStreamKey	Grants permission to get multiple stream keys simultaneously by stream key ARN	Read	Stream-Key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchStartViewerSessionRevocation	Grants permission to perform StartViewerSessionRevocation on multiple channel ARN and viewer ID pairs simultaneously	Write	Channel*		
CreateChannel	Grants permission to create a new channel and an associated stream key	Write	Channel*		
			Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEncoderConfiguration	Grants permission to create a new encoder configuration	Write	Encoder-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIngestConfiguration	Grants permission to create a new ingest configuration	Write	Ingest-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateParticipantToken	Grants permission to create a participant token	Write	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePlaybackRestrictionPolicy	Grants permission to create a playback restriction policy	Write	Playback-Restriction-Policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRecordingConfiguration	Grants permission to create a a new recording configuration	Write	Recording-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStage	Grants permission to create a stage	Write	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStorageConfiguration	Grants permission to create a new storage configuration	Write	Storage-Configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamKey	Grants permission to create a stream key	Write	Stream-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChannel	Grants permission to delete a channel and channel's stream keys	Write	Channel*		
			Stream-Key*		
DeleteEncoderConfiguration	Grants permission to delete an encoder configuration for the specified ARN	Write	Encoder-Configuration*		
DeleteIngestConfiguration	Grants permission to delete an ingest configuration for the specified ARN	Write	Ingest-Configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePlaybackKeyPair	Grants permission to delete the playback key pair for a specified ARN	Write	Playback-Key-Pair*		
DeletePlaybackRestrictionPolicy	Grants permission to delete the playback restriction policy for a specified ARN	Write	Playback-Restriction-Policy*		
DeletePublicKey	Grants permission to delete the public key for the specified ARN	Write	Public-Key*		
DeleteRecordingConfiguration	Grants permission to delete a recording configuration for the specified ARN	Write	Recording-Configuration*		
DeleteStage	Grants permission to delete the stage for a specified ARN	Write	Stage*		
DeleteStorageConfiguration	Grants permission to delete an storage configuration for the specified ARN	Write	Storage-Configuration*		
DeleteStreamKey	Grants permission to delete the stream key for a specified ARN	Write	Stream-Key*		
DisconnectParticipant	Grants permission to disconnect a participant from for the specified stage ARN	Write	Stage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetChannel	Grants permission to get the channel configuration for a specified channel ARN	Read	Channel*		
GetComposition	Grants permission to get the composition for the specified ARN	Read	Composition*		
GetEncoderConfiguration	Grants permission to get the encoder configuration for the specified ARN	Read	Encoder-Configuration*		
GetIngestConfiguration	Grants permission to get the ingest configuration for the specified ARN	Read	Ingest-Configuration*		
GetParticipant	Grants permission to get participant information for a specified stage ARN, session, and participant	Read	Stage*		
GetPlaybackKeyPair	Grants permission to get the playback keypair information for a specified ARN	Read	Playback-Key-Pair*		
GetPlaybackRestrictionPolicy	Grants permission to get the playback restriction policy for a specified ARN	Read	Playback-Restriction-Policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPublicKey	Grants permission to get the public key for the specified ARN	Read	Public-Key*		
GetRecordingConfiguration	Grants permission to get the recording configuration for the specified ARN	Read	Recording-Configuration*		
GetStage	Grants permission to get stage information for a specified ARN	Read	Stage*		
GetStageSession	Grants permission to get stage session information for a specified stage ARN and session	Read	Stage*		
GetStorageConfiguration	Grants permission to get the storage configuration for the specified ARN	Read	Storage-Configuration*		
GetStream	Grants permission to get information about the active (live) stream on a specified channel	Read	Channel*		
GetStreamKey	Grants permission to get stream-key information for a specified ARN	Read	Stream-Key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStreamSession	Grants permission to get information about the stream session on a specified channel	Read	Channel*		
ImportPlaybackKeyPair	Grants permission to import the public key	Write	Playback-Key-Pair*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportPublicKey	Grants permission to import a public key	Write	Public-Key*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListChannels	Grants permission to get summary information about channels	List	Channel*		
ListCompositions	Grants permission to get summary information about compositions	List	Encoder-Configuration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Stage		
ListEncoderConfigurations	Grants permission to get summary information about encoder configurations	List			
ListIngestConfigurations	Grants permission to get summary information about ingest configurations	List			
ListParticipantEvents	Grants permission to list participant events for a specified stage ARN, session, and participant	List	Stage*		
ListParticipantReplicas	Grants permission to get summary information about participant replicas	List	Stage*		
ListParticipants	Grants permission to list participants for a specified stage ARN and session	List	Stage*		
ListPlaybackKeyPairs	Grants permission to get summary information about playback key pairs	List	Playback-Key-Pair*		
ListPlaybackRestrictionPolicies	Grants permission to get summary information about playback restriction policies	List			
ListPublicKeys	Grants permission to get summary information about public keys	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecordingConfigurations	Grants permission to get summary information about recording configurations	List	Recording-Configuration*		
ListStageSessions	Grants permission to list stage sessions for a specified stage ARN	List	Stage*		
ListStages	Grants permission to get summary information about stages	List	Stage*		
ListStorageConfigurations	Grants permission to get summary information about storage configurations	List			
ListStreamKeys	Grants permission to get summary information about stream keys	List	Channel*		
			Stream-Key*		
ListStreamSessions	Grants permission to get summary information about streams sessions on a specified channel	List	Channel*		
ListStreams	Grants permission to get summary information about live streams	List	Channel*		
ListTagsForResource	Grants permission to get information about the tags for a specified ARN	Read	Channel		
			Composition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
PutMetadata	Grants permission to insert metadata into an RTMP stream for a specified channel	Write	Channel*		
StartComposition	Grants permission to start a new composition	Write	Encoder-Configuration*		
			Stage*		
			Channel		
			Storage-Configuration		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartParticipantReplication	Grants permission to start a new participant replication	Write	Stage*		
				aws:TagKeys aws:RequestTag/${TagKey}	
StartViewerSessionRevocation	Grants permission to start the process of revoking the viewer session associated with a specified channel ARN and viewer ID	Write	Channel*		
StopComposition	Grants permission to stop the composition for the specified ARN	Write	Composition*		
StopParticipantReplication	Grants permission to stop the participant replication for the specified ARN	Write	Stage*		
StopStream	Grants permission to disconnect a streamer on a specified channel	Write	Channel*		
TagResource	Grants permission to add or update tags for a resource with a specified ARN	Tagging	Channel		
			Composition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags for a resource with a specified ARN	Tagging	Channel		
			Composition		
			Encoder-Configuration		
			Ingest-Configuration		
			Playback-Key-Pair		
			Playback-Restriction-Policy		
			Public-Key		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Recording-Configuration		
			Stage		
			Storage-Configuration		
			Stream-Key		
				aws:TagKeys	
UpdateChannel	Grants permission to update a channel's configuration	Write	Channel*		
UpdateIngestConfiguration	Grants permission to update ingest configuration for a specified ARN	Write	Ingest-Configuration*		
UpdatePlaybackRestrictionPolicy	Grants permission to update a playback restriction policy for a specified ARN	Write	Playback-Restriction-Policy*		
UpdateStage	Grants permission to update a stage's configuration	Write	Stage*		

Resource types defined by Amazon Interactive Video 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
Channel	`arn:${Partition}:ivs:${Region}:${Account}:channel/${ResourceId}`	aws:ResourceTag/${TagKey}
Stream-Key	`arn:${Partition}:ivs:${Region}:${Account}:stream-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Key-Pair	`arn:${Partition}:ivs:${Region}:${Account}:playback-key/${ResourceId}`	aws:ResourceTag/${TagKey}
Playback-Restriction-Policy	`arn:${Partition}:ivs:${Region}:${Account}:playback-restriction-policy/${ResourceId}`	aws:ResourceTag/${TagKey}
Recording-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:recording-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}
Stage	`arn:${Partition}:ivs:${Region}:${Account}:stage/${ResourceId}`	aws:ResourceTag/${TagKey}
Composition	`arn:${Partition}:ivs:${Region}:${Account}:composition/${ResourceId}`	aws:ResourceTag/${TagKey}
Encoder-Configuration	`arn:${Partition}:ivs:${Region}:${Account}:encoder-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Storage-Configuration	arn:${Partition}:ivs:${Region}:${Account}:storage-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
Public-Key	arn:${Partition}:ivs:${Region}:${Account}:public-key/${ResourceId}	aws:ResourceTag/${TagKey}
Ingest-Configuration	arn:${Partition}:ivs:${Region}:${Account}:ingest-configuration/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Interactive Video Service

Amazon Interactive Video Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags associated with the request	String
aws:ResourceTag/${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 Interactive Video Service Chat

Amazon Interactive Video Service Chat (service prefix: `ivschat`) 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 Interactive Video Service Chat

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateChatToken	Grants permission to create an encrypted token that is used to establish an individual WebSocket connection to a room	Write	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoggingConfiguration	Grants permission to create a logging configuration that allows clients to record room messages	Write	Logging-Configuration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoom	Grants permission to create a room that allows clients to connect and pass messages	Write	Room*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLoggingConfiguration	Grants permission to delete the logging configuration for a specified logging configuration ARN	Write	Logging-Configuration*		
DeleteMessage	Grants permission to send an event to a specific room which directs clients to delete a specific message	Write	Room*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoom	Grants permission to delete the room for a specified room ARN	Write	Room*		
DisconnectUser	Grants permission to disconnect all connections using a specified user ID from a room	Write	Room*		
GetLoggingConfiguration	Grants permission to get the logging configuration for a specified logging configuration ARN	Read	Logging-Configuration*		
GetRoom	Grants permission to get the room configuration for a specified room ARN	Read	Room*		
ListLoggingConfigurations	Grants permission to get summary information about logging configurations	List	Logging-Configuration*		
ListRooms	Grants permission to get summary information about rooms	List	Room*		
ListTagsForResource	Grants permission to get information about the tags for a specified ARN	Read	Room		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
SendEvent	Grants permission to send an event to a room	Write	Room*		
TagResource	Grants permission to add or update tags for a resource with a specified ARN	Tagging	Logging-Configuration		
			Room		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags for a resource with a specified ARN	Tagging	Logging-Configuration		
			Room		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateLoggingConfiguration	Grants permission to update the logging configuration for a specified logging configuration ARN	Write	Logging-Configuration*		
UpdateRoom	Grants permission to update the room configuration for a specified room ARN	Write	Room*		

Resource types defined by Amazon Interactive Video Service Chat

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
Room	`arn:${Partition}:ivschat:${Region}:${Account}:room/${ResourceId}`	aws:ResourceTag/${TagKey}
Logging-Configuration	`arn:${Partition}:ivschat:${Region}:${Account}:logging-configuration/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Interactive Video Service Chat

Amazon Interactive Video Service Chat defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags associated with the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Interconnect

AWS Interconnect (service prefix: `interconnect`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Interconnect
- Resource types defined by AWS Interconnect
- Condition keys for AWS Interconnect

Actions defined by AWS Interconnect

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptConnectionProposal	Grants permission to accept a connection proposal generated elsewhere	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Grants permission to create a connection	Write	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteConnection	Grants permission to delete an existing connection	Write	connection*		
DescribeConnectionProposal	Grants permission to describe a connection proposal	Read			
GetConnection	Grants permission to describe a connection	Read	connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEnvironment	Grants permission to describe an environment	Read	environment*		
ListAttachPoints	Grants permission to list available attach points	Read			
ListConnections	Grants permission to list connections	List			
ListEnvironments	Grants permission to list available environments	List			
ListTagsForResource	Grants permission to list tags on a resource	Read			
TagResource	Grants permission to apply tags to a resource	Tagging	connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	connection*		
				aws:TagKeys	
UpdateConnection	Grants permission to update an existing connection	Write	connection*		

Resource types defined by AWS Interconnect

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:${Partition}:interconnect:${Region}:${Account}:connection/${Id}`	aws:ResourceTag/${TagKey}
environment	`arn:${Partition}:interconnect:${Region}:${Account}:environment/${Id}`	

Condition keys for AWS Interconnect

AWS Interconnect defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Invoicing Service

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateProcurementPortalPreference	Grants permission to create a procurement portal preference	Write		aws:ResourceTag/${TagKey}	
DeleteInvoiceUnit	Grants permission to update an invoice unit for your organization	Write	invoice-unit*		
				aws:ResourceTag/${TagKey}	
DeleteProcurementPortalPreference	Grants permission to delete a procurement portal preference	Write		aws:ResourceTag/${TagKey}	
GetInvoiceCorrection [permission only]	Grants permission to get Invoice Correction	Read			
GetInvoiceEmailDeliveryPreferences [permission only]	Grants permission to get Invoice Email Delivery Preferences	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInvoicePDF	Grants permission to get downloadable Invoice document pre-signed URL with supplemental documents	Read			
GetInvoiceUnit	Grants permission to get invoice units for your organization	Read	invoice-unit*		
GetProcurementPortalPreference	Grants permission to get a procurement portal preference	Read			
ListInvoiceCorrections [permission only]	Grants permission to list Invoice Corrections	List			
ListInvoiceSummaries	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			
ListProcurementPortalPreferences	Grants permission to list procurement portal preferences for an account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a resource	Read	invoice-unit*		
				aws:ResourceTag/${TagKey}	
PutInvoiceEmailDeliveryPreferences [permission only]	Grants permission to put Invoice Email Delivery Preferences	Write			
PutProcurementPortalPreference	Grants permission to update a procurement portal preference	Write		aws:ResourceTag/${TagKey}	
StartInvoiceCorrection [permission only]	Grants permission to start Invoice Correction	Write			
TagResource	Grants permission to tag a resource	Tagging	invoice-unit*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	invoice-unit*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	Grants permission to update an invoice unit for your organization	Write	invoice-unit*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProcurementPortalPreferenceStatus	Grants permission to update the status for a procurement portal preference	Write		aws:ResourceTag/${TagKey}	

Resource types defined by AWS 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}
procurement-portal-preference	`arn:${Partition}:invoicing::${Account}:procurement-portal-preference/${Identifier}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Invoicing Service

AWS 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 AWS 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 AWS IoT

AWS 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 AWS IoT
- Resource types defined by AWS IoT
- Condition keys for AWS IoT

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	
CreatePolicy	Grants permission to create an AWS IoT policy	Permissions management	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyVersion	Grants permission to create a new version of the specified AWS IoT policy	Permissions management	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 AWS 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		
DeleteConnection	Grants permission to disconnect the specified connection	Write	client*		
DeleteCustomMetric	Grants permission to deletes the specified custom metric from your AWS account	Write	custommetric*		
DeleteDimension	Grants permission to remove the specified dimension from your AWS 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 AWS 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	Permissions management	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicyVersion	Grants permission to Delete the specified version of the specified policy	Permissions management	policy*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteThing	Grants permission to delete the specified thing	Write	thing*		
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 AWS 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 AWS 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
DescribeEncryptionConfiguration	Grants permission to describe the encryption configuration for the account	Read			
DescribeEndpoint	Grants permission to get a unique endpoint specific to the AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeManagedJobTemplate	Grants permission to describe a managed job template	Read	jobtemplate*		
DescribeMitigationAction	Grants permission to get information about a mitigation action	Read	mitigationaction*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dimension		
			thinggroup		
DetachThingPrincipal	Grants permission to detach the specified principal from the specified thing	Write	cert		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetThingShadow	Grants permission to get the thing shadow	Read	thing*		
GetTopicRule	Grants permission to get information about the specified rule	Read	rule*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAuditMitigationActionsTasks	Grants permission to get a list of audit mitigation action tasks that match the specified filters	List			
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 AWS account	List			
ListCertificateProviders	Grants permission to list certificate providers in the account	List			
ListCertificates	Grants permission to list your certificates	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCertificatesByCA	Grants permission to list the device certificates signed by the specified CA certificate	List			
ListCommandExecutions	Grants permission to list commands executions in the account	List	client		
			command		
			thing		
ListCommands	Grants permission to list commands in the account	List			
ListCustomMetrics	Grants permission to list the custom metrics in your AWS 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 AWS account	List			
ListDomainConfigurations	Grants permission to list the domain configuration created by your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFleetMetrics	Grants permission to list the fleet metrics in your account	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNamedShadowsForThing	Grants permission to list all named shadows for a given thing	List	thing*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRoleAliases	Grants permission to list role aliases	List			
ListSbomValidationResults	Grants permission to list SBOM validation results of a package version	List	packageversion*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			command		
			custommetric		
			dimension		
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		
			job		
			jobtemplate		
			mitigationaction		
			otaupdate		
			policy		
			provisioningtemplate		
			rolealias		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rule		
			scheduledaudit		
			securityprofile		
			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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListThingPrincipalsV2	Grants permission to list the principals associated with the specified thing	List	thing*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTunnels	Grants permission to list tunnels	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Receive	Grants permission to receive from the specified topic	Write	topic*		
RegisterCACertificate	Grants permission to register a CA certificate with AWS IoT	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	iam:PassRole
RegisterCertificate	Grants permission to register a device certificate with AWS IoT	Write			
RegisterCertificateWithoutCA	Grants permission to register a device certificate with AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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
			scheduled audit		
			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 AWS 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*		
UpdateEncryptionConfiguration	Grants permission to update the encryption configuration for the account	Write			
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 AWS 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/${TagKey}
scheduledaudit	arn:${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 AWS IoT

AWS 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 AWS 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 AWS IoT Analytics

AWS 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 AWS IoT Analytics
- Resource types defined by AWS IoT Analytics
- Condition keys for AWS IoT Analytics

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchPutMessage	Puts a batch of messages into the specified channel	Write	channel*		
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 AWS 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 AWS IoT Analytics

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:TagKeys	Filters access based on the presence of tag keys in the request	ArrayOfString
iotanalytics:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String

Actions, resources, and condition keys for AWS IoT Core Device Advisor

AWS IoT Core Device Advisor (service prefix: `iotdeviceadvisor`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS IoT Core Device 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSuiteDefinition	Grants permission to create a suite definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSuiteDefinition	Grants permission to delete a suite definition	Write	Suitedefinition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEndpoint	Grants permission to get a Device Advisor endpoint	Read			
GetSuiteDefinition	Grants permission to get a suite definition	Read	Suitedefinition*		
GetSuiteRun	Grants permission to get a suite run	Read	Suiterun*		
GetSuiteRunReport	Grants permission to get the qualification report for a suite run	Read	Suiterun*		
ListSuiteDefinitions	Grants permission to list suite definitions	List			
ListSuiteRuns	Grants permission to list suite runs	List	Suitedefinition*		
ListTagsForResource	Grants permission to list the tags (metadata) assigned to a resource	Read	Suitedefinition Suiterun		
StartSuiteRun	Grants permission to start a suite run	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopSuiteRun	Grants permission to stop a suite run	Write	Suiterun*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add to or modify the tags of the given resource. Tags are metadata which can be used to manage a resource	Tagging	Suitedefinition		
			Suiterun		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the given tags (metadata) from a resource	Tagging	Suitedefinition		
			Suiterun		
				aws:TagKeys	
UpdateSuiteDefinition	Grants permission to update a suite definition	Write	Suitedefinition*		

Resource types defined by AWS IoT Core Device 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.

Resource types	ARN	Condition keys
Suitedefinition	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suitedefinition/${SuiteDefinitionId}`	aws:ResourceTag/${TagKey}
Suiterun	`arn:${Partition}:iotdeviceadvisor:${Region}:${Account}:suiterun/${SuiteDefinitionId}/${SuiteRunId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS IoT Core Device Advisor

AWS IoT Core Device Advisor defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS IoT Device Tester

AWS IoT Device Tester (service prefix: `iot-device-tester`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS IoT Device Tester

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckVersion	Grants permission to IoT Device Tester to check if a given set of product, test suite and device tester version are compatible	Read			
DownloadTestSuite	Grants permission to IoT Device Tester to download compatible test suite versions	Read			
LatestIdt	Grants permission to IoT Device Tester to get informati	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	on on latest version of device tester available				
SendMetrics	Grants permission to IoT Device Tester to send usage metrics on your behalf	Write			
Supported Version	Grants permission to IoT Device Tester to get list of supported products and test suite versions	Read			

Resource types defined by AWS IoT Device Tester

AWS IoT Device Tester does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS IoT Device Tester, specify `"Resource": "*"` in your policy.

Condition keys for AWS IoT Device Tester

IoT Device Tester has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS IoT Events

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAcknowledgeAlarm	Grants permission to send one or more acknowledge action requests to AWS IoT Events	Write	alarmModel*		
BatchDeleteDetector	Grants permission to delete a detector instance within the AWS 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*		
BatchPutMessage	Grants permission to send a set of messages to the AWS IoT Events system	Write	input*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS IoT Events system	Write	detectorModel*		
CreateAlarmModel	Grants permission to create an alarm model to monitor an AWS IoT Events input attribute or an AWS IoT SiteWise asset property	Write	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorModel	Grants permission to create a detector model to monitor an AWS IoT Events input attribute	Write	detectorModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribeDetector	Grants permission to retriev information about a detector instance	Read	detectorModel*		
DescribeDetectorModel	Grants permission to retrieve information about a detector model	Read	detectorModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS IoT Events logging options	Write			
StartDetectorModelAnalysis	Grants permission to start the detector model analysis	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateDetectorModel	Grants permission to update a detector model	Write	detectorModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInput	Grants permission to update an input	Write	input*		
UpdateInputRouting	Grants permission to update input routing	Write	input*		

Resource types defined by AWS 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 AWS IoT Events

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to the resource	String
aws:TagKeys	Filters 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 AWS IoT Fleet Hub for Device Management

AWS IoT Fleet Hub for Device Management (service prefix: `iotfleethub`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IoT Fleet Hub for Device Management

- Resource types defined by AWS IoT Fleet Hub for Device Management
- Condition keys for AWS IoT Fleet Hub for Device Management

Actions defined by AWS IoT Fleet Hub for Device Management

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
DeleteApplication	Grants permission to delete an application	Write	application*		sso:DeleteManagedApplicationInstance
DescribeApplication	Grants permission to describe an application	Read	application*		
ListApplications	Grants permission to list all applications	List			
ListTagsForResource	Grants permission to list all tags for a resource	Read	application		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging	application		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	application		
				aws:TagKeys	
UpdateApplication	Grants permission to update an application	Write	application*		

Resource types defined by AWS IoT Fleet Hub for Device 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
application	`arn:${Partition}:iotfleethub:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS IoT Fleet Hub for Device Management

AWS IoT Fleet Hub for Device Management defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
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

Actions, resources, and condition keys for AWS IoT FleetWise

AWS IoT FleetWise (service prefix: `iotfleetwise`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS IoT FleetWise

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateVehicleFleet	Grants permission to associate the given vehicle to a fleet	Write	fleet*		
			vehicle*		
CreateCampaign	Grants permission to create a campaign	Write	campaign*		
			fleet*		
			signalcatalog*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iotfleetwise:DestinationArn	
CreateDecoderManifest	Grants permission to create a decoder manifest for an existing model	Write	decodermanifest*		
			modelmanifest*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFleet	Grants permission to create a fleet	Write	fleet*		
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelManifest	Grants permission to create a model manifest definition	Write	modelmanifest*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSignalCatalog	Grants permission to create a signal catalog	Write	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateTemplate	Grants permission to create a state template	Write	signalcatalog*		
			statetemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVehicle	Grants permission to create a vehicle	Write	decodermanifest*		iot:CreateThing iot:DescribeThing
			modelmanifest*		
			vehicle*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCampaign	Grants permission to delete a campaign	Write	campaign*		
DeleteDecoderManifest	Grants permission to delete the given decoder manifest	Write	decodermanifest*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFleet	Grants permission to delete a fleet	Write	fleet*		
DeleteModelManifest	Grants permission to delete the given model manifest	Write	modelmanifest*		
DeleteSignalCatalog	Grants permission to delete a specific signal catalog	Write	signalcatalog*		
DeleteStateTemplate	Grants permission to delete a state template	Write	statetemplate*		
DeleteVehicle	Grants permission to delete a vehicle	Write	vehicle*		
DisassociateVehicleFleet	Grants permission to disassociate a vehicle from an existing fleet	Write	fleet*		
			vehicle*		
GenerateCommandPayload [permission only]	Grants permission to generate the payload for running a command on a vehicle	Permissions management	vehicle*		
			statetemplate		
				iotfleetwise:Signals	
GetCampaign	Grants permission to get summary information for a given campaign	Read	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDecoderManifest	Grants permission to get summary information for a given decoder manifest definition	Read	decodermanifest*		
GetEncryptionConfiguration	Grants permission to get KMS-based encryption status for the AWS account	Read			
GetFleet	Grants permission to get summary information for a fleet	Read	fleet*		
GetLoggingOptions	Grants permission to get the logging options for the AWS account	Read			
GetModelManifest	Grants permission to get summary information for a given model manifest definition	Read	modelmanifest*		
GetRegisterAccountStatus	Grants permission to get the account registration status with IoT FleetWise	Read			
GetSignalCatalog	Grants permission to get summary information for a specific signal catalog	Read	signalcatalog*		
GetStateTemplate	Grants permission to get summary information for a given state template	Read	statetemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVehicle	Grants permission to get summary information for a vehicle	Read	vehicle*		
GetVehicleStatus	Grants permission to get the status of the campaigns running on a specific vehicle	Read	vehicle*		
ImportDecoderManifest	Grants permission to import an existing decoder manifest	Write	decodermanifest*		
ImportSignalCatalog	Grants permission to create a signal catalog by importing existing definitions	Write	signalcatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCampaigns	Grants permission to list campaigns	Read			
ListDecoderManifestNetworkInterfaces	Grants permission to list network interfaces associated to the existing decoder manifest	List	decodermanifest*		
ListDecoderManifestSignals	Grants permission to list decoder manifest signals	List	decodermanifest*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDecoderManifests	Grants permission to list all decoder manifests, with an optional filter on model manifest	Read			
ListFleets	Grants permission to list all fleets	Read			
ListFleetsForVehicle	Grants permission to list all the fleets that the given vehicle is associated with	Read	vehicle*		
ListModelManifestNodes	Grants permission to list all nodes for the given model manifest	List	modelmanifest*		
ListModelManifests	Grants permission to list all model manifests, with an optional filter on signal catalog	Read			
ListSignalCatalogNodes	Grants permission to list all nodes for a given signal catalog	Read	signalcatalog*		
ListSignalCatalogs	Grants permission to list all signal catalogs	Read			
ListStateTemplates	Grants permission to list state templates	Read			
ListTagsForResource	Grants permission to list tags for a resource	Read	campaign		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
ListVehicles	Grants permission to list all vehicles, with an optional filter on model manifest	Read			
ListVehiclesInFleet	Grants permission to list vehicles in the given fleet	Read	fleet*		
PutEncryptionConfiguration	Grants permission to enable or disable KMS-based encryption for the AWS account	Write			
PutLoggingOptions	Grants permission to put the logging options for the AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterAccount	Grants permission to register an AWS account to IoT FleetWise	Write			iam:PassRole
TagResource	Grants permission to add tags to a resource	Tagging	campaign		
			decodermanifest		
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	campaign		
			decodermanifest		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet		
			modelmanifest		
			signalcatalog		
			statetemplate		
			vehicle		
				aws:TagKeys	
UpdateCampaign	Grants permission to update the given campaign	Write	campaign*		
UpdateDecoderManifest	Grants permission to update a decoder manifest defnition	Write	decodermanifest*		
UpdateFleet	Grants permission to update the fleet	Write	fleet*		
UpdateModelManifest	Grants permission to update the given model manifest definition	Write	modelmanifest*		
UpdateSignalCatalog	Grants permission to update a specific signal catalog definition	Write	signalcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStateTemplate	Grants permission to update the given state template	Write	statetemplate*		
UpdateVehicle	Grants permission to update the vehicle	Write	vehicle*		
			decodermanifest		
			modelmanifest		
				iotfleetwise:UpdateToModelManifestArn iotfleetwise:UpdateToDecoderManifestArn	

Resource types defined by AWS IoT FleetWise

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
campaign	arn:${Partition}:iotfleetwise:${Region}:${Account}:campaign/${CampaignName}	aws:ResourceTag/${TagKey}
decodermanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:decoder-manifest/${Name}	aws:ResourceTag/${TagKey}
fleet	arn:${Partition}:iotfleetwise:${Region}:${Account}:fleet/${FleetId}	aws:ResourceTag/${TagKey}
modelmanifest	arn:${Partition}:iotfleetwise:${Region}:${Account}:model-manifest/${Name}	aws:ResourceTag/${TagKey}
signalcatalog	arn:${Partition}:iotfleetwise:${Region}:${Account}:signal-catalog/${Name}	aws:ResourceTag/${TagKey}
vehicle	arn:${Partition}:iotfleetwise:${Region}:${Account}:vehicle/${VehicleId}	aws:ResourceTag/${TagKey}
statetemplate	arn:${Partition}:iotfleetwise:${Region}:${Account}:state-template/${StateTemplateId}	aws:ResourceTag/${TagKey}

Condition keys for AWS IoT FleetWise

AWS IoT FleetWise defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
iotfleetwise:DestinationArn	Filters access by campaign destination ARN, eg. an S3 bucket ARN or a Timestream ARN	ARN
iotfleetwise:Signals	Filters access by fully qualified signal names	ArrayOfString
iotfleetwise:UpdateToDecoderManifestArn	Filters access by a list of IoT FleetWise Decoder Manifest ARNs	ARN
iotfleetwise:UpdateToModelManifestArn	Filters access by a list of IoT FleetWise Model Manifest ARNs	ARN

Actions, resources, and condition keys for AWS IoT Greengrass

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS services	Write	group*		
AssociateServiceRoleToAccount	Grants permission to associate a role with your account. AWS IoT Greengrass uses this role to access your Lambda functions and AWS IoT resources	Permissions management			
CreateConnectorDefinition	Grants permission to create a connector definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	Grants permission to create a version of an existing core definition. Greengrass groups must each contain exactly one Greengrass core	Write	coreDefinition*		
CreateDeployment	Grants permission to create a deployment	Write	group*		
CreateDeviceDefinition	Grants permission to create a device definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	Grants permission to create a version of an existing device definition	Write	deviceDefinition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	
CreateFunctionDefinitionVersion	Grants permission to create a version of an existing Lambda function definition	Write	functionDefinition*		
CreateGroup	Grants permission to create a group	Write		aws:RequestTag/${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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoggerDefinition	Grants permission to create a logger definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	Grants permission to create a version of an existing logger definition	Write	loggerDefinition*		
CreateResourceDefinition	Grants permission to create a resource definition that contains a list of resources to be used in a group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDefinitionVersion	Grants permission to create a version of an existing resource definition	Write	resourceDefinition*		
CreateSoftwareUpdateJob	Grants permission to create an AWS IoT job that will trigger your Greengrass cores to update the software they are running	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DeleteResourceDefinition	Grants permission to delete a resource definition	Write	resourceDefinition*		
DeleteSubscription Definition	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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListTagsForResource	Grants permission to list the tags for a resource	Read	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a resource	Tagging	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	
UntagResource	Grants permission to remove tags from a resource	Tagging	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateThingRuntimeConfiguration	Grants permission to update runtime configuration of a thing	Write	thingRuntimeConfig*		

Resource types defined by AWS 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/${TagKey}
group	arn:${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}	

Resource types	ARN	Condition keys
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}	
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}

Resource types	ARN	Condition keys
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}
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 AWS IoT Greengrass

AWS 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 AWS 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 AWS IoT Greengrass V2

AWS 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 AWS IoT Greengrass V2
- Resource types defined by AWS IoT Greengrass V2
- Condition keys for AWS IoT Greengrass V2

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateServiceRoleToAccount	Grants permission to associate a role with your account. AWS IoT Greengrass uses this role to access your Lambda functions and AWS IoT resources	Permissions management			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	Grants permission to associate a list of client devices with a core device	Write	coreDevice*		
BatchDisassociateClientDeviceFromCoreDevice	Grants permission to disassociate a list of client devices from a core device	Write	coreDevice*		
CancelDeployment	Grants permission to cancel a deployment	Write	deployment*		iot:CancelJob iot:DeleteThingShadow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	Grants permission to create a component	Write	component * 		
				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 AWS IoT Greengrass core device, which is an AWS IoT thing. This operation removes the core device from the list of core devices. This operation doesn't delete the AWS 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 AWS 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 AWS 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 AWS 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 AWS IoT Greengrass sends to AWS 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 AWS 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 AWS 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 AWS IoT Greengrass V2

AWS 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 AWS 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 AWS IoT Jobs DataPlane

AWS 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 AWS IoT Jobs DataPlane
- Resource types defined by AWS IoT Jobs DataPlane
- Condition keys for AWS IoT Jobs DataPlane

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJobExecution	Grants permission to describe a job execution	Read	thing*		
				iot:JobId	
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 AWS 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 AWS IoT Jobs DataPlane

AWS 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 AWS 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 AWS IoT Managed Integrations

AWS IoT Managed Integrations (service prefix: `iotmanagedintegrations`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IoT Managed Integrations
- Resource types defined by AWS IoT Managed Integrations
- Condition keys for AWS IoT Managed Integrations

Actions defined by AWS IoT Managed Integrations

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccountAssociation	Grants permission to create a new account association	Write		aws:RequestTag/${TagKey} aws:TagKeys iotmanagedintegrations:connectorDestinationId	
CreateCloudConnector	Grants permission to create a new cloud connector	Write			
CreateConnectorDestination	Grants permission to create a new connector destination	Write		iotmanagedintegrations:cloudConnectorId	
CreateCredentialLocker	Grants permission to create a product credential locker	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDestination	Grants permission to create a new destination	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventLogConfiguration	Grants permission to create a new event configuration	Write			
CreateManagedThing	Grants permission to create a new managed thing	Write	credential-locker		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationConfiguration	Grants permission to create a new notification configuration	Write			
CreateOtaTask	Grants permission to create a new ota task	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOtaTaskConfiguration	Grants permission to create a new ota task configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProvisioningProfile	Grants permission to create a new provisioning profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssociation	Grants permission to delete an account association	Write	account-association*		
DeleteCloudConnector	Grants permission to delete a cloud connector	Write		iotmanagedintegrations:cloudConnectorId	
DeleteConnectorDestination	Grants permission to delete a connector destination	Write			
DeleteCredentialLocker	Grants permission to delete a credential locker	Write	credential-locker*		
DeleteDestination	Grants permission to delete destination	Write			
DeleteEventLogConfiguration	Grants permission to delete event log configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteManagedThing	Grants permission to delete managed thing	Write	managed-thing*		
DeleteNotificationConfiguration	Grants permission to delete notification configuration	Write			
DeleteOtaTask	Grants permission to delete ota task	Write	ota-task*		
DeleteOtaTaskConfiguration	Grants permission to delete ota task configuration	Write			
DeleteProvisioningProfile	Grants permission to delete provisioning profile	Write	provisioning-profile*		
DeregisterAccountAssociation	Grants permission to deregister account association	Write	account-association*		
			managed-thing*		
GetAccountAssociation	Grants permission to get information about an account association	Read	account-association*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCloudConnector	Grants permission to get information about a cloud connector	Read			
GetConnectorDestination	Grants permission to get information about a cloud destination	Read			
GetCredentialLocker	Grants permission to get information about a credential locker	Read	credential-locker*		
GetCustomEndpoint	Grants permission to get information about a custom endpoint	Read			
GetDefaultEncryptionConfiguration	Grants permission to get information about a default encryption configuration	Read			
GetDestination	Grants permission to get information about a destination	Read			
GetDeviceDiscovery	Grants permission to get information about a device discovery	Read			
GetEventLogConfiguration	Grants permission to get information about an event log configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHubConfiguration	Grants permission to get information about a hub configuration	Read			
GetManagedThing	Grants permission to get information about a managed thing	Read	managed-thing*		
GetManagedThingCapabilities	Grants permission to get the capability report for a managed thing	Read	managed-thing*		
GetManagedThingCertificate	Grants permission to get the certificate pem for a managed thing	Read	managed-thing*		
GetManagedThingConnectivityData	Grants permission to get the connectivity data for a managed thing	Read	managed-thing*		
GetManagedThingMetaData	Grants permission to get the meta data information for a managed thing	Read	managed-thing*		
GetManagedThingState	Grants permission to get the device state information for a managed thing	Read	managed-thing*		
GetNotificationConfiguration	Grants permission to get information for a notification configuration	Read			
GetOtaTask	Grants permission to get information for an ota task	Read	ota-task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOtaTaskConfiguration	Grants permission to get information for an ota task configuration	Read			
GetProvisioningProfile	Grants permission to get information for a provisioning profile	Read	provisioning-profile*		
GetRuntimeLogConfiguration	Grants permission to get information for a runtime log configuration	Read			
GetSchemaVersion	Grants permission to get information for a version of a schema	Read			
ListAccountAssociations	Grants permission to list information for account associations	List			
ListCloudConnectors	Grants permission to list information for cloud connectors	List			
ListConnectorDestinations	Grants permission to list information for connector destinations	List			
ListCredentialLockers	Grants permission to list information for credential lockers	List			
ListDestinations	Grants permission to list information for destinations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeviceDiscoveries	Grants permission to list information for device discoveries	List			
ListDiscoveredDevices	Grants permission to list information for device discovered in a device discoveries	Read			
ListEventLogConfigurations	Grants permission to list information for event log configurations	Read			
ListManagedThingAccountAssociations	Grants permission to list information for associations between managed thing and account associations	List			
ListManagedThingSchemas	Grants permission to list schemas associated with a managed thing	Read	managed-thing*		
ListManagedThings	Grants permission to list information for managed things	List			
ListNotificationConfigurations	Grants permission to list information for notification configurations	Read			
ListOtaTaskConfigurations	Grants permission to list information for ota task configurations	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOtaTaskExecutions	Grants permission to list information for ota task executions	Read	ota-task*		
ListOtaTasks	Grants permission to list information for ota tasks	List			
ListProvisioningProfiles	Grants permission to list information for provisioning profiles	List			
ListSchemaVersions	Grants permission to list information for schemas	List			
ListTagsForResource	Grants permission to list tags for the specified resource	Read	account-association		
			credential-locker		
			managed-thing		
			ota-task		
			provisioning-profile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
PutDefaultEncryptionConfiguration	Grants permission to update the default settings for an encryption configuration	Write			
PutHubConfiguration	Grants permission to update a hub configuration	Write			
PutRuntimeLogConfiguration	Grants permission to update a runtime log configuration	Write			
RegisterAccountAssociation	Grants permission to register an account association to a managed thing	Write	account-association*		
			managed-thing*		
RegisterCustomEndpoint	Grants permission to register a custom endpoint	Write			
ResetRuntimeLogConfiguration	Grants permission to reset a runtime log configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendConnectorEvent	Grants permission to send a connector event	Write			
SendManagedThingCommand	Grants permission to send a command to a managed thing	Write	managed-thing*		
			account-association		
StartAccountAssociationRefresh	Grants permission to start a refresh of access tokens associated with an account association	Write	account-association*		
StartDeviceDiscovery	Grants permission to start a device discovery	Write	account-association		
			managed-thing		
TagResource	Grants permission to add tags for the specified resource	Tagging	account-association		
			credential-locker		
			managed-thing		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ota-task		
			provisioning-profile		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags for the specified resource	Tagging	account-association		
			credential-locker		
			managed-thing		
			ota-task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			provisioning-profile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateAccountAssociation	Grants permission to update an account association	Write	account-association*		
UpdateCloudConnector	Grants permission to update a cloud connector	Write		iotmanagedintegrations:cloudConnectorId	
UpdateConnectorDestination	Grants permission to update a connector destination	Write			
UpdateDestination	Grants permission to update a destination	Write			
UpdateEventLogConfiguration	Grants permission to update an event log configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateManagedThing	Grants permission to update a managed thing	Write	managed-thing*		
			credential-locker		
UpdateNotificationConfiguration	Grants permission to update a notification configuration	Write			
UpdateOtaTask	Grants permission to update an ota task	Write	ota-task*		

Resource types defined by AWS IoT Managed Integrations

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-association	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:account-association/${AccountAssociationId}`	aws:ResourceTag/${TagKey}
credential-locker	`arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:credential-locker/${Identifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
managed-thing	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:managed-thing/${Identifier}	aws:ResourceTag/${TagKey}
ota-task	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:ota-task/${Identifier}	aws:ResourceTag/${TagKey}
provisioning-profile	arn:${Partition}:iotmanagedintegrations:${Region}:${Account}:provisioning-profile/${Identifier}	aws:ResourceTag/${TagKey}

Condition keys for AWS IoT Managed Integrations

AWS IoT Managed Integrations defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString
iotmanagedintegrat	Filters access by the CloudConnectorId	String

Condition keys	Description	Type
ions:clou dConnectorId		
iotmanage dintegrat ions:conn ectorDest inationId	Filters access by the ConnectorDestinationId	String

Actions, resources, and condition keys for AWS IoT SiteWise

AWS 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 AWS IoT SiteWise
- Resource types defined by AWS IoT SiteWise
- Condition keys for AWS IoT SiteWise

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAssets	Grants permission to associate a child asset with a parent asset through a hierarchy	Write	asset*		
AssociateTimeSeriesToAssetProperty	Grants permission to associate a time series with an asset property	Write	asset* 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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	Grants permission to create an asset from an asset model	Write	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAssetModel	Grants permission to create an asset model	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModelCompositeModel	Grants permission to create an asset model composite model inside an asset model	Write	asset-model*		
CreateBulkImportJob	Grants permission to create bulk import job	Write			
CreateComputationModel	Grants permission to create a computation model	Write	asset		
			asset-model		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Grants permission to create a dashboard in a project	Write	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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/${TagKey} aws:TagKeys	
CreatePortal	Grants permission to create a portal	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DeleteAssetModelInterfaceRelationship	Grants permission to delete a relationship between asset model and interface	Write	asset-model*		
DeleteComputationModel	Grants permission to delete a computation model	Write	computation-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		
			computation-model		
DescribeAsset	Grants permission to describe an asset	Read	asset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAssetCompositeModel	Grants permission to describe an asset composite model	Read	asset*		
DescribeAssetModel	Grants permission to describe an asset model	Read	asset-model*		
DescribeAssetModelCompositeModel	Grants permission to describe an asset model composite model	Read	asset-model*		
DescribeAssetModelInterfaceRelationship	Grants permission to describe a relationship between asset model and interface	Read	asset-model*		
DescribeAssetProperty	Grants permission to describe an asset property	Read	asset*		
DescribeBulkImportJob	Grants permission to describe bulk import job	Read			
DescribeComputationModel	Grants permission to describe a computation model	Read	computation-model*		
DescribeComputationModelExecutionSummary	Grants permission to describe computation model execution summary	Read	computation-model*		
			asset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account	Read			
DescribeExecution	Grants permission to describe an execution	Read			
DescribeGateway	Grants permission to describe a gateway	Read	gateway*		
DescribeGatewayCapabilityConfiguration	Grants permission to describe a capability configuration for a gateway	Read	gateway*		
DescribeLoggingOptions	Grants permission to describe logging options for the AWS account	Read			
DescribePortal	Grants permission to describe a portal	Read	portal*		
DescribeProject	Grants permission to describe a project	Read	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStorageConfiguration	Grants permission to describe the storage configuration for the AWS 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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			computation-model		
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		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListActions	Grants permission to list all actions	List	asset		
			computation-model		
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCompositionRelationships	Grants permission to list all asset model composition relationships	List	asset-model*		
ListComputationModelDataBindingUsages	Grants permission to list computation model data binding usages	List	asset		
			asset-model		
ListComputationModelResolveToResources	Grants permission to list computation model resolve to resources	List	computation-model*		
ListComputationModels	Grants permission to list all computation models	List			
ListDashboards	Grants permission to list all dashboards in a project	List	project*		
ListDatasets	Grants permission to list all datasets	List			
ListExecutions	Grants permission to list executions	List	asset		
			computation-model		
ListGateways	Grants permission to list all gateways	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInterfaceRelationships	Grants permission to list all asset models that are enforced by an interface	List	asset-model*		
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*		
ListTagsForResource	Grants permission to list all tags for a resource	Read	access-policy		
			asset		
			asset-model		
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	Grants permission to list time series	List	asset		
PutAssetModelInterfaceRelationship	Grants permission to create a relationship between asset model and interface	Write	asset-model*		
PutDefaultEncryptionConfiguration	Grants permission to set the default encryption configuration for the AWS account	Write			
PutLoggingOptions	Grants permission to set logging options for the AWS account	Write			
PutStorageConfiguration	Grants permission to configure storage settings for the AWS account	Write			
TagResource	Grants permission to tag a resource	Tagging	access-policy		
			asset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			asset-model		
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	access-policy		
			asset		
			asset-model		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			computation-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	Grants permission to update an access policy	Write	access-policy*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAssetModelPropertyRouting [permission only]	Grants permission to update an AssetModel property routing	Write	asset-model*		
UpdateAssetProperty	Grants permission to update an asset property	Write	asset*		
UpdateComputationModel	Grants permission to update a computation model	Write	computation-model*		
			asset		
			asset-model		
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*		
UpdatePortal	Grants permission to update a portal	Write	portal*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProject	Grants permission to update a project	Write	project*		

Resource types defined by AWS 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}
portal	`arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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}
computation-model	arn:${Partition}:iotsitewise:${Region}:${Account}:computation-model/${ComputationModelId}	aws:ResourceTag/${TagKey}

Condition keys for AWS IoT SiteWise

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to the resource	String

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 AWS Single Sign-On group	String
iotsitewise:iam	Filters access by the ID of an AWS 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 AWS Single Sign-On user	String

Actions, resources, and condition keys for AWS IoT TwinMaker

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchPutPropertyValues	Grants permission to set values for multiple time series properties	Write	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			entity		
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 AWS 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 AWS IoT TwinMaker

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to the resource	String
aws:TagKeys	Filters access by the tag keys in 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 AWS IoT Wireless

AWS IoT Wireless (service prefix: `iotwireless`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IoT Wireless
- Resource types defined by AWS IoT Wireless
- Condition keys for AWS IoT Wireless

Actions defined by AWS IoT Wireless

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateAwsAccountWithPartnerAccount	Grants permission to link partner accounts with AWS account	Write		aws:RequestTag/${TagKey} aws:TagKeys	
AssociateMulticastGroupWithFuotaTask	Grants permission to associate the MulticastGroup with FuotaTask	Write	FuotaTask* MulticastGroup*		
AssociateWirelessDeviceWithFuotaTask	Grants permission to associate the wireless device with FuotaTask	Write	FuotaTask* WirelessDevice*		
AssociateWirelessDeviceWithMulticastGroup	Grants permission to associate the WirelessDevice with MulticastGroup	Write	MulticastGroup* WirelessDevice*		
AssociateWirelessD	Grants permission to associate the wireless device	Write	WirelessDevice*		iot:DescribeThing

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
eviceWithThing	with AWS IoT thing for a given wirelessDeviceId		thing*		
AssociateWirelessGatewayWithCertificate	Grants permission to associate a WirelessGateway with the IoT Core Identity certificate	Write	WirelessGateway*		
			cert*		
AssociateWirelessGatewayWithThing	Grants permission to associate the wireless gateway with AWS IoT thing for a given wirelessGatewayId	Write	WirelessGateway*		iot:DescribeThing
			thing*		
CancelMulticastGroupSession	Grants permission to cancel the MulticastGroup session	Write	MulticastGroup*		
CreateDestination	Grants permission to create a Destination resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceProfile	Grants permission to create a DeviceProfile resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFuotaTask	Grants permission to create a FuotaTask resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMulticastGroup	Grants permission to create a MulticastGroup resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNetworkAnalyzerConfiguration	Grants permission to create a NetworkAnalyzerConfiguration resource	Write	MulticastGroup*		
			WirelessDevice*		
			WirelessGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServiceProfile	Grants permission to create a ServiceProfile resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessDevice	Grants permission to create a WirelessDevice resource with given Destination	Write	Destination		
			DeviceProfile		
			ServiceProfile		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWirelessGateway	Grants permission to create a WirelessGateway resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWirelessGatewayTask	Grants permission to create a task for a given WirelessGateway	Write	WirelessGateway*		
CreateWirelessGatewayTaskDefinition	Grants permission to create a WirelessGateway task definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDestination	Grants permission to delete a Destination	Write	Destination*		
DeleteDeviceProfile	Grants permission to delete a DeviceProfile	Write	DeviceProfile*		
DeleteFuotaTask	Grants permission to delete the FuotaTask	Write	FuotaTask*		
DeleteMulticastGroup	Grants permission to delete the MulticastGroup	Write	MulticastGroup*		
DeleteNetworkAnalyzerConfiguration	Grants permission to delete the NetworkAnalyzerConfiguration	Write	NetworkAnalyzerConfiguration*		
DeleteQueuedMessages	Grants permission to delete QueuedMessages	Write			
DeleteServiceProfile	Grants permission to delete a ServiceProfile	Write	ServiceProfile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWirelessDevice	Grants permission to delete a WirelessDevice	Write	WirelessDevice*		
DeleteWirelessDeviceImportTask	Grants permission to delete the wireless device import task	Write	ImportTask*		
DeleteWirelessGateway	Grants permission to delete a WirelessGateway	Write	WirelessGateway*		
DeleteWirelessGatewayTask	Grants permission to delete task for a given WirelessGateway	Write	WirelessGateway*		
DeleteWirelessGatewayTaskDefinition	Grants permission to delete a WirelessGateway task definition	Write	WirelessGatewayTaskDefinition*		
DeregisterWirelessDevice	Grants permission to deregister wireless device	Write	WirelessDevice*		
DisassociateAwsAccountFromPartnerAccount	Grants permission to disassociate an AWS account from a partner account	Write	SidewalkAccount*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateMulticastGroupFromFuotaTask	Grants permission to disassociate the MulticastGroup from FuotaTask	Write	FuotaTask*		
			MulticastGroup*		
DisassociateWirelessDeviceFromFuotaTask	Grants permission to disassociate the wireless device from FuotaTask	Write	FuotaTask*		
			WirelessDevice*		
DisassociateWirelessDeviceFromMulticastGroup	Grants permission to disassociate the wireless device from MulticastGroup	Write	MulticastGroup*		
			WirelessDevice*		
DisassociateWirelessDeviceFromThing	Grants permission to disassociate a wireless device from a AWS IoT thing	Write	WirelessDevice*		iot:DescribeThing
			thing*		
DisassociateWirelessGatewayFromCertificate	Grants permission to disassociate a WirelessGateway from a IoT Core Identity certificate	Write	WirelessGateway*		
			cert*		
DisassociateWirelessGatewayFromThing	Grants permission to disassociate a WirelessGateway from a IoT Core thing	Write	WirelessGateway*		iot:DescribeThing
			thing*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDestination	Grants permission to get the Destination	Read	Destination*		
GetDeviceProfile	Grants permission to get the DeviceProfile	Read	DeviceProfile*		
GetEventConfigurationByResourceTypes	Grants permission to get event configuration by resource types	Read			
GetFuotaTask	Grants permission to get the FuotaTask	Read	FuotaTask*		
GetLogLevelsByResourceTypes	Grants permission to get log levels by resource types	Read			
GetMetricConfiguration	Grants permission to get metric configuration	Read			
GetMetrics	Grants permission to get metrics	Read			
GetMulticastGroup	Grants permission to get the MulticastGroup	Read	MulticastGroup*		
GetMulticastGroupSession	Grants permission to get the MulticastGroup session	Read	MulticastGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetworkAnalyzerConfiguration	Grants permission to get the NetworkAnalyzerConfiguration	Read	NetworkAnalyzerConfiguration*		
GetPartnerAccount	Grants permission to get the associated PartnerAccount	Read	SidewalkAccount*		
GetPosition	Grants permission to get position for a given resource	Read	WirelessDevice		
			WirelessGateway		
GetPositionConfiguration	Grants permission to get position configuration for a given resource	Read	WirelessDevice		
			WirelessGateway		
GetPositionEstimate	Grants permission to get position estimate	Read			
GetResourceEventConfiguration	Grants permission to get an event configuration for an identifier	Read	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
GetResourceLogLevel	Grants permission to get resource log level	Read	WirelessDevice		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			WirelessGateway		
GetResourcePosition	Grants permission to get position for a given resource	Read	WirelessDevice		
			WirelessGateway		
GetServiceEndpoint	Grants permission to retrieve the customer account specific endpoint for CUPS protocol connection or LoRaWAN Network Server (LNS) protocol connection, and optionally server trust certificate in PEM format	Read			
GetServiceProfile	Grants permission to get the ServiceProfile	Read	ServiceProfile*		
GetWirelessDevice	Grants permission to get the WirelessDevice	Read	WirelessDevice*		
GetWirelessDeviceImportTask	Grants permission to get the wireless device import task	Read	ImportTask*		
GetWirelessDeviceStatistics	Grants permission to get statistics info for a given WirelessDevice	Read	WirelessDevice*		
GetWirelessGateway	Grants permission to get the WirelessGateway	Read	WirelessGateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWirelessGatewayCertificate	Grants permission to get the IoT Core Identity certificate id associated with the WirelessGateway	Read	WirelessGateway*		
GetWirelessGatewayFirmwareInformation	Grants permission to get Current firmware version and other information for the WirelessGateway	Read	WirelessGateway*		
GetWirelessGatewayStatistics	Grants permission to get statistics info for a given WirelessGateway	Read	WirelessGateway*		
GetWirelessGatewayTask	Grants permission to get the task for a given WirelessGateway	Read	WirelessGateway*		
GetWirelessGatewayTaskDefinition	Grants permission to get the given WirelessGateway task definition	Read	WirelessGatewayTaskDefinition*		
ListDestinations	Grants permission to list information of available Destinations based on the AWS account	Read			
ListDeviceProfiles	Grants permission to list information of available DeviceProfiles based on the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDevicesForWirelessDeviceImportTask	Grants permission to list information of devices by wireless device import task based on the AWS account	Read	ImportTask*		
ListEventConfigurations	Grants permission to list information of available event configurations based on the AWS account	Read			
ListFuotaTasks	Grants permission to list information of available FuotaTasks based on the AWS account	Read			
ListMulticastGroups	Grants permission to list information of available MulticastGroups based on the AWS account	Read			
ListMulticastGroupsByFuotaTask	Grants permission to list information of available MulticastGroups by FuotaTask based on the AWS account	Read	FuotaTask*		
ListNetworkAnalyzerConfigurations	Grants permission to list information of available NetworkAnalyzerConfigurations based on the AWS account	Read			
ListPartnerAccounts	Grants permission to list the available partner accounts	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPositionConfigurations	Grants permission to list information of available position configurations based on the AWS account	Read			
ListQueuedMessages	Grants permission to list the Queued Messages	Read			
ListServiceProfiles	Grants permission to list information of available ServiceProfiles based on the AWS account	Read			
ListTagsForResource	Grants permission to list all tags for a given resource	Read	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
ListWirelessDeviceImportTasks	Grants permission to list wireless device import tasks information of based on the AWS account	Read			
ListWirelessDevices	Grants permission to list information of available WirelessDevices based on the AWS account	Read			
ListWirelessGatewayTaskDefinitions	Grants permission to list information of available WirelessGateway task definitions based on the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWirelessGateways	Grants permission to list information of available WirelessGateways based on the AWS account	Read			
PutPositionConfiguration	Grants permission to put position configuration for a given resource	Write	WirelessDevice		
			WirelessGateway		
PutResourceLogLevel	Grants permission to put resource log level	Write	WirelessDevice		
			WirelessGateway		
ResetAllResourceLogLevels	Grants permission to reset all resource log levels	Write			
ResetResourceLogLevel	Grants permission to reset resource log level	Write	WirelessDevice		
			WirelessGateway		
SendDataToMulticastGroup	Grants permission to send data to the MulticastGroup	Write	MulticastGroup*		
SendDataToWirelessDevice	Grants permission to send the decrypted application data frame to the target device	Write	WirelessDevice*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartBulkAssociateWirelessDeviceWithMulticastGroup	Grants permission to associate the WirelessDevices with MulticastGroup	Write	MulticastGroup*		
StartBulkDisassociateWirelessDeviceFromMulticastGroup	Grants permission to bulk disassociate the WirelessDevices from MulticastGroup	Write	MulticastGroup*		
StartFuotaTask	Grants permission to start the FuotaTask	Write	FuotaTask*		
StartMulticastGroupSession	Grants permission to start the MulticastGroup session	Write	MulticastGroup*		
StartNetworkAnalyzerStream	Grants permission to start NetworkAnalyzer stream	Write	NetworkAnalyzerConfiguration*		
StartSingleWirelessDeviceImportTask	Grants permission to start the single wireless device import task	Write	Destination		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
StartWirelessDeviceImportTask	Grants permission to start the wireless device import task	Write	ImportTask*		
			Destination		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to tag a given resource	Tagging	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestWirelessDevice	Grants permission to simulate a provisioned device to send an uplink data with payload of 'Hello'	Write	WirelessDevice*		
UntagResource	Grants permission to remove the given tags from the resource	Tagging	Destination		
			DeviceProfile		
			FuotaTask		
			ImportTask		
			MulticastGroup		
			NetworkAnalyzerConfiguration		
			ServiceProfile		
			SidewalkAccount		
			WirelessDevice		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			WirelessGateway		
			WirelessGatewayTaskDefinition		
				aws:TagKeys	
UpdateDestination	Grants permission to update a Destination resource	Write	Destination*		
UpdateEventConfigurationByResourceTypes	Grants permission to update event configuration by resource types	Write			
UpdateFuotaTask	Grants permission to update the FuotaTask	Write	FuotaTask*		
UpdateLogLevelsByResourceTypes	Grants permission to update log levels by resource types	Write			
UpdateMetricConfiguration	Grants permission to update metric configuration	Write			
UpdateMulticastGroup	Grants permission to update the MulticastGroup	Write	MulticastGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNetworkAnalyzerConfiguration	Grants permission to update the NetworkAnalyzerConfiguration	Write	MulticastGroup*		
			NetworkAnalyzerConfiguration*		
			WirelessDevice*		
			WirelessGateway*		
UpdatePartnerAccount	Grants permission to update a partner account	Write	SidewalkAccount*		
UpdatePosition	Grants permission to update position for a given resource	Write	WirelessDevice		
			WirelessGateway		
UpdateResourceEventConfiguration	Grants permission to update an event configuration for an identifier	Write	SidewalkAccount		
			WirelessDevice		
			WirelessGateway		
UpdateResourcePosition	Grants permission to update position for a given resource	Write	WirelessDevice		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			WirelessGateway		
UpdateWirelessDevice	Grants permission to update a WirelessDevice resource	Write	WirelessDevice*		
			Destination		
			DeviceProfile		
			ServiceProfile		
UpdateWirelessDeviceImportTask	Grants permission to update a wireless device import task	Write	ImportTask*		
UpdateWirelessGateway	Grants permission to update a WirelessGateway resource	Write	WirelessGateway*		

Resource types defined by AWS IoT Wireless

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
WirelessDevice	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessDevice/${WirelessDeviceId}	aws:ResourceTag/${TagKey}
WirelessGateway	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGateway/${WirelessGatewayId}	aws:ResourceTag/${TagKey}
DeviceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:DeviceProfile/${DeviceProfileId}	aws:ResourceTag/${TagKey}
ServiceProfile	arn:${Partition}:iotwireless:${Region}:${Account}:ServiceProfile/${ServiceProfileId}	aws:ResourceTag/${TagKey}
Destination	arn:${Partition}:iotwireless:${Region}:${Account}:Destination/${DestinationName}	aws:ResourceTag/${TagKey}
SidewalkAccount	arn:${Partition}:iotwireless:${Region}:${Account}:SidewalkAccount/${SidewalkAccountId}	aws:ResourceTag/${TagKey}
WirelessGatewayTaskDefinition	arn:${Partition}:iotwireless:${Region}:${Account}:WirelessGatewayTaskDefinition/${WirelessGatewayTaskDefinitionId}	aws:ResourceTag/${TagKey}
FuotaTask	arn:${Partition}:iotwireless:${Region}:${Account}:FuotaTask/${FuotaTaskId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Multicast Group	arn:${Partition}:iotwireless:${Region}:${Account}:MulticastGroup/${MulticastGroupId}	aws:ResourceTag/${TagKey}
NetworkAnalyzerConfiguration	arn:${Partition}:iotwireless:${Region}:${Account}:NetworkAnalyzerConfiguration/${NetworkAnalyzerConfigurationName}	aws:ResourceTag/${TagKey}
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
cert	arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}	
ImportTask	arn:${Partition}:iotwireless:${Region}:${Account}:ImportTask/${ImportTaskId}	aws:ResourceTag/${TagKey}

Condition keys for AWS IoT Wireless

AWS IoT Wireless defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key that is present in the request that the user makes to IoT Wireless	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key component of a tag attached to an IoT Wireless resource	String
aws:TagKeys	Filters access by the list of all the tag key names associated with the resource in the request	ArrayOfString
iotwireless:DestinationName	Filters access by destination name associated with the IoT Wireless resource	String
iotwireless:DeviceProfileId	Filters access by device profile id associated with the IoT Wireless resource	String
iotwireless:ServiceProfileId	Filters access by service profile id associated with the IoT Wireless resource	String

Actions, resources, and condition keys for AWS IQ

AWS IQ (service prefix: `iq`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IQ
- Resource types defined by AWS IQ
- Condition keys for AWS IQ

Actions defined by AWS IQ

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptCall	Grants permission to accept an incoming voice/video call	Write	call*		
ApprovePaymentRequest	Grants permission to approve a payment request	Write	paymentRequest*		
ApproveProposal	Grants permission to approve a proposal	Write	proposal*		
ArchiveConversation	Grants permission to archive a conversation	Write	conversation*		
CompleteProposal	Grants permission to complete a proposal	Write	proposal*		
CreateConversation	Grants permission to respond to a request or send a direct message to initiate a conversation	Write			
CreateExpert	Grants permission to create an expert profile	Write			
CreateListing	Grants permission to create a listing	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMilestoneProposal	Grants permission to create a milestone proposal	Write			
CreatePaymentRequest	Grants permission to create a payment request	Write			
CreateProject	Grants permission to submit new requests	Write			
CreateRequest	Grants permission to submit new requests	Write			
CreateScheduledProposal	Grants permission to create a scheduled proposal	Write			
CreateSeller	Grants permission to create a seller profile	Write			
CreateUpfrontProposal	Grants permission to create an upfront proposal	Write			
DeclineCall	Grants permission to decline an incoming voice/video call	Write	call*		
DeleteAttachment	Grants permission to delete an existing attachment	Write	attachment*		
DisableIndividualPublicProfile	Grants permission to disable individual public profile page	Write	expert*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DownloadAttachment	Grants permission to download existing attachment	Read	attachment*		
EnableIndividualPublicProfile	Grants permission to enable individual public profile page	Write	expert*		
EndCall	Grants permission to end a voice/video call	Write	call*		
GetBuyer	Grants permission to read buyer information	Read	buyer*		
GetCall	Grants permission to read details of a voice/video call	Read	call*		
GetChatInfo	Grants permission to read the chat environment details about a conversation	Read	conversation*		
GetChatMessages	Grants permission to read chat messages in a conversation	Read	conversation*		
GetChatToken	Grants permission to request a websocket token for the conversation notifications	Read	token*		
GetCompanyChatMessages	Grants permission to read chat messages in a company conversation	Read	conversation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCompanyProfile	Grants permission to read a company profile	Read	company*		
GetConversation	Grants permission to read details of a conversation	Read	conversation*		
GetExpert	Grants permission to read expert information	Read	expert*		
GetListing	Grants permission to read a listing	Read	listing*		
GetMarketplaceSeller	Grants permission to read a seller profile information	Read	seller*		
GetPaymentRequest	Grants permission to read a payment request	Read	paymentRequest*		
GetProposal	Grants permission to read a proposal	Read	proposal*		
GetRequest	Grants permission to get a created request	Read	request*		
GetReview	Grants permission to read a review for an expert	Read	seller*		
HideRequest	Grants permission to hide a request	Write	request*		
InitiateCall	Grants permission to start a voice/video call	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LinkAwsCertification	Grants permission to link an AWS certification to individual profile	Write	expert*		
ListAttachments	Grants permission to list existing attachments	List	attachment*		
ListConversations	Grants permission to list existing conversations	Read	conversation*		
ListExpertAccessLogs	Grants permission to list access logs of expert activity	Read	permission*		
ListListings	Grants permission to list listings	Read	listing*		
ListPaymentRequests	Grants permission to list payment requests	Read	paymentRequest		
			paymentSchedule		
ListProposals	Grants permission to list proposals	Read	proposal*		
ListRequests	Grants permission to list requests that are created	Read	request*		
ListReviews	Grants permission to list reviews for an expert	Read	seller*		
MarkChatMessageRead	Grants permission to mark a message as read in a conversation	Write	conversation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectPaymentRequest	Grants permission to reject a payment request	Write	paymentRequest*		
RejectProposal	Grants permission to reject a proposal	Write	proposal*		
SendCompanyChatMessage	Grants permission to send a message in a conversation as a company	Write	conversation*		
SendIndividualChatMessage	Grants permission to send a message in a conversation as an individual	Write	conversation*		
UnarchiveConversation	Grants permission to unarchive a conversation	Write	conversation*		
UnlinkAwsCertification	Grants permission to unlink an AWS certification from individual profile	Write	expert*		
UpdateCompanyProfile	Grants permission to update a company profile	Write	company*		
UpdateConversationMembers	Grants permission to add more participants into a conversation	Write	conversation*		
UpdateExpert	Grants permission to update an expert information	Write	expert*		
UpdateListing	Grants permission to update a listing	Write	listing*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRequest	Grants permission to update a request	Write	request*		
UploadAttachment	Grants permission to upload an attachment	Write			
WithdrawPaymentRequest	Grants permission to withdraw a payment request	Write	paymentRequest*		
WithdrawProposal	Grants permission to withdraw a proposal	Write	proposal*		
WriteReview	Grants permission to write a review for an expert	Write	seller*		

Resource types defined by AWS IQ

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
conversation	`arn:${Partition}:iq:${Region}::conversation/${ConversationId}`	
buyer	`arn:${Partition}:iq:${Region}::buyer/${BuyerId}`	

Resource types	ARN	Condition keys
expert	arn:${Partition}:iq:${Region}::expert/${ExpertId}	
call	arn:${Partition}:iq:${Region}::call/${CallId}	
token	arn:${Partition}:iq:${Region}::token/${TokenId}	
proposal	arn:${Partition}:iq:${Region}::proposal/${ConversationId}/${ProposalId}	
paymentRequest	arn:${Partition}:iq:${Region}::paymentRequest/${ConversationId}/${ProposalId}/${PaymentRequestId}	
paymentSchedule	arn:${Partition}:iq:${Region}::paymentSchedule/${ConversationId}/${ProposalId}/${VersionId}	
seller	arn:${Partition}:iq:${Region}::seller/${SellerAwsAccountId}	
company	arn:${Partition}:iq:${Region}::company/${CompanyId}	
request	arn:${Partition}:iq:${Region}::request/${RequestId}	
listing	arn:${Partition}:iq:${Region}::listing/${ListingId}	
attachment	arn:${Partition}:iq:${Region}::attachment/${AttachmentId}	

Resource types	ARN	Condition keys
permission	arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}	

Condition keys for AWS IQ

IQ has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS IQ Permissions

AWS IQ Permissions (service prefix: iq-permission) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IQ Permissions
- Resource types defined by AWS IQ Permissions
- Condition keys for AWS IQ Permissions

Actions defined by AWS IQ 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApproveAccessGrant	Grants permission to approve a permission request	Write	permission*		
ApprovePermissionRequest	Grants permission to approve a permission request	Write	permission*		
AssumePermissionRole	Grants permission to obtain a set of temporary security credentials for experts which they can use to access buyers' AWS resources	Write	permission*		
CreatePermissionRequest	Grants permission to create a permission request	Write	permission*		
GetPermissionRequest	Grants permission to get a permission request	Read	permission*		
ListPermissionRequests	Grants permission to list permission requests	Read	permission*		
RejectPermissionRequest	Grants permission to reject a permission request	Write	permission*		
RevokePermissionRequest	Grants permission to revoke a permission request which was previously approved	Write	permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
WithdrawPermissionRequest	Grants permission to withdraw a permission request that has not been approved or declined	Write	permission*		

Resource types defined by AWS IQ Permissions

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
permission	`arn:${Partition}:iq-permission:${Region}::permission/${PermissionRequestId}`	

Condition keys for AWS IQ Permissions

IQ Permission has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Kendra

Amazon Kendra (service prefix: `kendra`) 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 Kendra

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateEntitiesToExperience	Grants permission to put principal mapping in index	Write	experience*		
			index*		
AssociatePersonasToEntities	Defines the specific permissions of users or groups in your AWS SSO identity source with access to your Amazon Kendra experience	Write	experience*		
			index*		
BatchDeleteDocument	Grants permission to batch delete document	Write	index*		
BatchDeleteFeaturedResultsSet	Grants permission to delete a featured results set	Write	featured-results-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			index*		
BatchGetDocumentStatus	Grants permission to do batch get document status	Read	index*		
BatchPutDocument	Grants permission to batch put document	Write	index*		
ClearQuerySuggestions	Grants permission to clear out the suggestions for a given index, generated so far	Write	index*		
CreateAccessControlConfiguration	Grants permission to create an access control configuration	Write	index*		
CreateDataSource	Grants permission to create a data source	Write	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExperience	Creates an Amazon Kendra experience such as a search application	Write	index*		
CreateFaq	Grants permission to create an Faq	Write	index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeaturedResultsSet	Grants permission to create a featured results set	Write	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Grants permission to create an Index	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateQuerySuggestionsBlockList	Grants permission to create a QuerySuggestions BlockList	Write	index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThesaurus	Grants permission to create a Thesaurus	Write	index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessControlConfiguration	Grants permission to delete an access control configuration	Write	access-control-configuration*		
			index*		
DeleteDataSource	Grants permission to delete a data source	Write	data-source*		
			index*		
DeleteExperience	Deletes your Amazon Kendra experience such as a search application	Write	experience*		
			index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFaq	Grants permission to delete an Faq	Write	faq*		
			index*		
DeleteIndex	Grants permission to delete an Index	Write	index*		
DeletePrincipalMapping	Grants permission to delete principal mapping from index	Write	index*		
			data-source		
DeleteQuerySuggestionsBlockList	Grants permission to delete a QuerySuggestions BlockList	Write	index*		
			query-suggestions-block-list*		
DeleteThesaurus	Grants permission to delete a Thesaurus	Write	index*		
			thesaurus*		
DescribeAccessControlConfiguration	Grants permission to describe an access control configuration	Read	access-control-configuration*		
			index*		
DescribeDataSource	Grants permission to describe a data source	Read	data-source*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			index*		
DescribeExperience	Gets information about your Amazon Kendra experience such as a search application	Read	experience*		
			index*		
DescribeFaq	Grants permission to describe an Faq	Read	faq*		
			index*		
DescribeFeaturedResultsSet	Grants permission to describe a featured results set	Read	featured-results-set*		
			index*		
DescribeIndex	Grants permission to describe an Index	Read	index*		
DescribePrincipalMapping	Grants permission to describe principal mapping from index	Read	index*		
			data-source		
DescribeQuerySuggestionsBlockList	Grants permission to describe a QuerySuggestions BlockList	Read	index*		
			query-suggestions-block-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeQuerySuggestionsConfig	Grants permission to describe the query suggestions configuration for an index	Read	index*		
DescribeThesaurus	Grants permission to describe a Thesaurus	Read	index*		
			thesaurus*		
DisassociateEntitiesFromExperience	Prevents users or groups in your AWS SSO identity source from accessing your Amazon Kendra experience	Write	experience*		
			index*		
DisassociatePersonasFromEntities	Removes the specific permissions of users or groups in your AWS SSO identity source with access to your Amazon Kendra experience	Write	experience*		
			index*		
GetQuerySuggestions	Grants permission to get suggestions for a query prefix	Read	index*		
GetSnapshots	Retrieves search metrics data	Read	index*		
ListAccessControlConfigurations	Grants permission to list the access control configurations	List	index*		
ListDataSourceSyncJobs	Grants permission to get Data Source sync job history	List	data-source*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			index*		
ListDataSources	Grants permission to list the data sources	List	index*		
ListEntityPersonas	Lists specific permissions of users and groups with access to your Amazon Kendra experience	List	experience*		
			index*		
ListExperienceEntities	Lists users or groups in your AWS SSO identity source that are granted access to your Amazon Kendra experience	List	experience*		
			index*		
ListExperiences	Lists one or more Amazon Kendra experiences. You can create an Amazon Kendra experience such as a search application	List	index*		
ListFaqs	Grants permission to list the Faqs	List	index*		
ListFeaturedResultsSets	Grants permission to list the featured results sets	List	index*		
ListGroupsOlderThanOrderingId	Grants permission to list groups that are older than an ordering id	List	index*		
			data-source		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIndices	Grants permission to list the indexes	List			
ListQuerySuggestionsBlockLists	Grants permission to list the QuerySuggestions BlockLists	List	index*		
ListTagsForResource	Grants permission to list tags for a resource	Read	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		
ListThesauri	Grants permission to list the Thesauri	List	index*		
PutPrincipalMapping	Grants permission to put principal mapping in index	Write	index*		
			data-source		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Query	Grants permission to query documents and faqs	Read	index*		
Retrieve	Grants permission to retrieve relevant content from an index	Read	index*		
StartDataSourceSyncJob	Grants permission to start Data Source sync job	Write	data-source*		
			index*		
StopDataSourceSyncJob	Grants permission to stop Data Source sync job	Write	data-source*		
			index*		
SubmitFeedback	Grants permission to send feedback about a query results	Write	index*		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	data-source		
			faq		
			featured-results-set		
			index		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			query-suggestions-block-list		
			thesaurus		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	data-source		
			faq		
			featured-results-set		
			index		
			query-suggestions-block-list		
			thesaurus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAccessControlConfiguration	Grants permission to update an access control configuration	Write	access-control-configuration*		
			index*		
UpdateDataSource	Grants permission to update a data source	Write	data-source*		
			index*		
UpdateExperience	Updates your Amazon Kendra experience such as a search application	Write	index*		
UpdateFeaturedResultsSet	Grants permission to update a featured results set	Write	featured-results-set*		
			index*		
UpdateIndex	Grants permission to update an Index	Write	index*		
UpdateQuerySuggestionsBlockList	Grants permission to update a QuerySuggestions BlockList	Write	index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			query-suggestions-block-list*		
UpdateQuerySuggestionsConfig	Grants permission to update the query suggestions configuration for an index	Write	index*		
UpdateThesaurus	Grants permission to update a thesaurus	Write	index*		
			thesaurus*		

Resource types defined by Amazon Kendra

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:${Partition}:kendra:${Region}:${Account}:index/${IndexId}`	aws:ResourceTag/${TagKey}
data-source	`arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/data-source/${DataSourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
faq	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/faq/${FaqId}	aws:ResourceTag/${TagKey}
experience	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/experience/${ExperienceId}	
thesaurus	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/thesaurus/${ThesaurusId}	aws:ResourceTag/${TagKey}
query-suggestions-block-list	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/query-suggestions-block-list/${QuerySuggestionsBlockListId}	aws:ResourceTag/${TagKey}
featured-results-set	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/featured-results-set/${FeaturedResultsSetId}	aws:ResourceTag/${TagKey}
access-control-configuration	arn:${Partition}:kendra:${Region}:${Account}:index/${IndexId}/access-control-configuration/${AccessControlConfigurationId}	

Condition keys for Amazon Kendra

Amazon Kendra defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking (service prefix: `kendra-ranking`) 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 Kendra Intelligent Ranking

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRescoreExecutionPlan	Grants permission to create a RescoreExecutionPlan	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteRescoreExecutionPlan	Grants permission to delete a RescoreExecutionPlan	Write	rescore-execution-plan*		
DescribeRescoreExecutionPlan	Grants permission to describe a RescoreExecutionPlan	Read	rescore-execution-plan*		
ListRescoreExecutionPlans	Grants permission to list all RescoreExecutionPlans	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	rescore-execution-plan		
Rescore	Grants permission to Rescore documents with Kendra Intelligent Ranking	Read	rescore-execution-plan*		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	rescore-execution-plan		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	rescore-execution-plan		
				aws:TagKeys	
UpdateRescoreExecutionPlan	Grants permission to update a RescoreExecutionPlan	Write	rescore-execution-plan*		

Resource types defined by Amazon Kendra Intelligent Ranking

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
rescore-execution-plan	`arn:${Partition}:kendra-ranking:${Region}:${Account}:rescore-execution-plan/${RescoreExecutionPlanId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Kendra Intelligent Ranking

Amazon Kendra Intelligent Ranking defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Key Management Service

AWS Key Management Service (service prefix: `kms`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Key Management Service

- Resource types defined by AWS Key Management Service
- Condition keys for AWS Key Management Service

Actions defined by AWS Key Management Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelKeyDeletion	Controls permission to cancel the scheduled deletion of an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
ConnectCustomKeyStore	Controls permission to connect or reconnect a custom key store to its associated AWS CloudHSM cluster or external key manager outside of AWS	Write		kms:CallerAccount	
CreateAlias	Controls permission to create an alias for an AWS KMS key. Aliases are optional friendly names that you can associate with KMS keys	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomKeyStore	Controls permission to create a custom key store that is backed by an AWS CloudHSM cluster or an external key manager outside of AWS	Write		kms:CallerAccount	cloudhsm:DescribeClusters ec2:DescribeVpcEndpointServices iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGrant	Controls permission to add a grant to an AWS KMS key. You can use grants to add permissions without changing the key policy or IAM policy	Permissions management	key*	kms:CallerAccount kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:GrantConstraintType kms:GranteePrincipal kms:GrantIsForAWSResource kms:GrantOperations kms:RetiringPrincipal	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKey	Controls permission to create an AWS KMS key that can be used to protect data keys and other sensitive information	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion	iam:CreateServiceLinkedRole kms:PutKeyPolicy kms:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:MultiRegionKeyType kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Decrypt	Controls permission to decrypt ciphertext that was encrypted under an AWS KMS key	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAlias	Controls permission to delete an alias. Aliases are optional friendly names that you can associate with AWS KMS keys	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	
DeleteCustomKeyStore	Controls permission to delete a custom key store	Write		kms:CallerAccount	
DeleteImportedKeyMaterial	Controls permission to delete cryptographic material that you imported into an AWS KMS key. This action makes the key unusable	Write	key*		
				kms:CallerAccount kms:ViaService	
DeriveSharedSecret	Controls permission to use the specified AWS KMS key to derive shared secrets	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:KeyAgreementAlgorithm kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:NitroTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6 kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:NitroTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17 kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:NitroTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	
DescribeCustomKeyStores	Controls permission to view detailed information about custom key stores in the account and region	Read		kms:CallerAccount	
DescribeKey	Controls permission to view detailed information about an AWS KMS key	Read	key*	kms:CallerAccount kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableKey	Controls permission to disable an AWS KMS key, which prevents it from being used in cryptographic operations	Write	key*		
				kms:CallerAccount kms:ViaService	
DisableKeyRotation	Controls permission to disable automatic rotation of a customer managed AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
DisconnectCustomKeyStore	Controls permission to disconnect the custom key store from its associated AWS CloudHSM cluster or external key manager outside of AWS	Write		kms:CallerAccount	
EnableKey	Controls permission to change the state of an AWS KMS key to enabled. This allows the KMS key to be used in cryptographic operations	Write	key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableKeyRotation	Controls permission to enable automatic rotation of the cryptographic material in an AWS KMS key	Write	key*		
				kms:CallerAccount kms:RotationPeriodInDays kms:ViaService	
Encrypt	Controls permission to use the specified AWS KMS key to encrypt data and data keys	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKey	Controls permission to use the AWS KMS key to generate data keys. You can use the data keys to encrypt data outside of AWS KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	
GenerateDataKeyPair	Controls permission to use the AWS KMS key to generate data key pairs	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:DataKeyPairSpec kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tation:NitroTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKeyPairWithoutPlaintext	Controls permission to use the AWS KMS key to generate data key pairs. Unlike the GenerateDataKeyPair operation, this operation returns an encrypted private key without a plaintext copy	Write	key*	kms:CallerAccount kms:DataKeyPairSpec kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKeyWithoutPlaintext	Controls permission to use the AWS KMS key to generate a data key. Unlike the GenerateDataKey operation, this operation returns an encrypted data key without a plaintext version of the data key	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	
GenerateMac	Controls permission to use the AWS KMS key to generate message authentication codes	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateRandom	Controls permission to get a cryptographically secure random byte string from AWS KMS	Write		kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:NitroTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6 kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:NitroTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17 kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:NitroTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR31	
GetKeyPolicy	Controls permission to view the key policy for the specified AWS KMS key	Read	key*		
				kms:CallerAccount kms:ViaService	
GetKeyRotationStatus	Controls permission to view the key rotation status for an AWS KMS key	Read	key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetParametersForImport	Controls permission to get data that is required to import cryptographic material into a customer managed key, including a public key and import token	Read	key*		
				kms:CallerAccount kms:ViaService kms:WrappingAlgorithm kms:WrappingKeySpec	
GetPublicKey	Controls permission to download the public key of an asymmetric AWS KMS key	Read	key*		
				kms:CallerAccount kms:RequestAlias kms:ViaService	
ImportKeyMaterial	Controls permission to import cryptographic material into an AWS KMS key	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:ExpirationModel kms:ValidTo kms:ViaService	
ListAliases	Controls permission to view the aliases that are defined in the account. Aliases are optional friendly names that you can associate with AWS KMS keys	List			
ListGrants	Controls permission to view all grants for an AWS KMS key	List	key*		
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	
ListKeyPolicies		List	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Controls permission to view the names of key policies for an AWS KMS key			kms:CallerAccount kms:ViaService	
ListKeyRotations	Controls permission to view the list of key materials for an AWS KMS key	List	key*		
				kms:CallerAccount kms:ViaService	
ListKeys	Controls permission to view the key ID and Amazon Resource Name (ARN) of all AWS KMS keys in the account	List			
ListResourceTags	Controls permission to view all tags that are attached to an AWS KMS key	List	key*		
				kms:CallerAccount kms:ViaService	
ListRetirableGrants	Controls permission to view grants in which the specified principal is the retiring principal. Other principals might be able to retire the grant and this principal might be able to retire other grants	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutKeyPolicy	Controls permission to replace the key policy for the specified AWS KMS key	Permissions management	key*		
				kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReEncryptFrom	Controls permission to decrypt data as part of the process that decrypts and reencrypts the data within AWS KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:ReEncryptOnSameKey kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReEncryptTo	Controls permission to encrypt data as part of the process that decrypts and reencrypts the data within AWS KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:ReEncryptOnSameKey kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplicateKey	Controls permission to replicate a multi-Region primary key	Write	key*		iam:CreateServiceLinkedRole kms:CreateKey kms:PutKeyPolicy kms:TagResource
				kms:CallerAccount kms:ReplicaRegion kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RetireGrant	Controls permission to retire a grant. The RetireGrant operation is typically called by the grant user after they complete the tasks that the grant allowed them to perform	Permissions management	key*		
				kms:CallerAccount kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:GrantConstraintType kms:ViaService	
RevokeGrant	Controls permission to revoke a grant, which denies permission for all operations that depend on the grant	Permissions management	key*		
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RotateKeyOnDemand	Controls permission to invoke on-demand rotation of the cryptographic material in an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
ScheduleKeyDeletion	Controls permission to schedule deletion of an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ScheduleKeyDeletionPendingWindowInDays kms:ViaService	
Sign	Controls permission to produce a digital signature for a message	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
SynchronizeMultiRegionKey [permission only]	Controls access to internal APIs that synchronize multi-Region keys	Write	key*		
TagResource	Controls permission to create or update tags that are attached to an AWS KMS key	Tagging	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys kms:CallerAccount kms:ViaService	
UntagResource	Controls permission to delete tags that are attached to an AWS KMS key	Tagging	key*		
				aws:TagKeys kms:CallerAccount kms:ViaService	
UpdateAlias	Controls permission to associate an alias with a different AWS KMS key. An alias is an optional friendly name that you can associate with a KMS key	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCustomKeyStore	Controls permission to change the properties of a custom key store	Write		kms:CallerAccount	ec2:DescribeVpcEndpointServices
UpdateKeyDescription	Controls permission to delete or change the description of an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
UpdatePrimaryRegion	Controls permission to update the primary Region of a multi-Region primary key	Write	key*		
				kms:CallerAccount kms:PrimaryRegion kms:ViaService	
Verify	Controls permission to use the specified AWS KMS key to verify digital signatures	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
VerifyMac	Controls permission to use the AWS KMS key to verify message authentication codes	Write	key*		
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	

Resource types defined by AWS Key Management Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types

that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
alias	`arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}`	
key	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	aws:ResourceTag/${TagKey} kms:KeyOrigin kms:KeySpec kms:KeyUsage kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases

Condition keys for AWS Key Management Service

AWS Key Management Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access to the specified AWS KMS operations based on both the key and value of the tag in the request	String
aws:ResourceTag/${TagKey}	Filters access to the specified AWS KMS operations based on tags assigned to the AWS KMS key	String
aws:TagKeys	Filters access to the specified AWS KMS operations based on tag keys in the request	ArrayOfString
kms:BypassPolicyLockoutSafetyCheck	Filters access to the CreateKey and PutKeyPolicy operations based on the value of the BypassPolicyLockoutSafetyCheck parameter in the request	Bool
kms:CallerAccount	Filters access to specified AWS KMS operations based on the AWS account ID of the caller. You can use this condition key to allow or deny access to all IAM users and roles in an AWS account in a single policy statement	String
kms:CustomerMasterKeySpec	The kms:CustomerMasterKeySpec condition key is deprecated. Instead, use the kms:KeySpec condition key	String
kms:CustomerMasterKeyUsage	The kms:CustomerMasterKeyUsage condition key is deprecated. Instead, use the kms:KeyUsage condition key	String
kms:DataKeyPairSpec	Filters access to GenerateDataKeyPair and GenerateDataKeyPairWithoutPlaintext operations based on the value of the KeyPairSpec parameter in the request	String
kms:EncryptionAlgorithm	Filters access to encryption operations based on the value of the encryption algorithm in the request	String

Condition keys	Description	Type
kms:EncryptionContext:${EncryptionContextKey}	Filters access to a symmetric AWS KMS key based on the encryption context in a cryptographic operation. This condition evaluates the key and value in each key-value encryption context pair	String
kms:EncryptionContextKeys	Filters access to a symmetric AWS KMS key based on the encryption context in a cryptographic operation. This condition key evaluates only the key in each key-value encryption context pair	ArrayOfString
kms:ExpirationModel	Filters access to the ImportKeyMaterial operation based on the value of the ExpirationModel parameter in the request	String
kms:GrantConstraintType	Filters access to the CreateGrant operation based on the grant constraint in the request	String
kms:GrantIsForAWSResource	Filters access to the CreateGrant operation when the request comes from a specified AWS service	Bool
kms:GrantOperations	Filters access to the CreateGrant operation based on the operations in the grant	ArrayOfString
kms:GranteePrincipal	Filters access to the CreateGrant operation based on the grantee principal in the grant	String
kms:KeyAgreementAlgorithm	Filters access to the DeriveSharedSecret operation based on the value of the KeyAgreementAlgorithm parameter in the request	String
kms:KeyOrigin	Filters access to an API operation based on the Origin property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key	String

Condition keys	Description	Type
kms:KeySpec	Filters access to an API operation based on the KeySpec property of the AWS KMS key that is created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	String
kms:KeyUsage	Filters access to an API operation based on the KeyUsage property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	String
kms:MacAlgorithm	Filters access to the GenerateMac and VerifyMac operations based on the MacAlgorithm parameter in the request	String
kms:MessageType	Filters access to the Sign and Verify operations based on the value of the MessageType parameter in the request	String
kms:MultiRegion	Filters access to an API operation based on the MultiRegion property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	Bool
kms:MultiRegionKeyType	Filters access to an API operation based on the MultiRegionKeyType property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	String
kms:PrimaryRegion	Filters access to the UpdatePrimaryRegion operation based on the value of the PrimaryRegion parameter in the request	String

Condition keys	Description	Type
kms:ReEncryptOnSameKey	Filters access to the ReEncrypt operation when it uses the same AWS KMS key that was used for the Encrypt operation	Bool
kms:RecipientAttestation:ImageSha384	Filters access to the API operations based on the image hash in the attestation document in the request	String
kms:RecipientAttestation:NitroTPMPCR0	Filters access by the platform configuration register (PCR) 0 in the attestation document in the request. PCR0 is a contiguous measure of core system firmware executable code	String
kms:RecipientAttestation:NitroTPMPCR1	Filters access by the platform configuration register (PCR) 1 in the attestation document in the request. PCR1 is a contiguous measure of core system firmware data/ host platform configuration, typically including serial and model numbers	String
kms:RecipientAttestation:NitroTPMPCR10	Filters access by the platform configuration register (PCR) 10 in the attestation document in the request. PCR10 is a contiguous measure of protection of the IMA measurement log	String
kms:RecipientAttestation:NitroTPMPCR11	Filters access by the platform configuration register (PCR) 11 in the attestation document in the request. PCR11 is a contiguous measure of all components of unified kernel images (UKIs)	String
kms:RecipientAttestation:NitroTPMPCR12	Filters access by the platform configuration register (PCR) 12 in the attestation document in the request. PCR12 is a contiguous measure of kernel command line, system credentials and system configuration images	String

Condition keys	Description	Type
kms:RecipientAttestation:NitroTPMPCR13	Filters access by the platform configuration register (PCR) 13 in the attestation document in the request. PCR13 is a contiguous measure of all system extension images for the initrd	String
kms:RecipientAttestation:NitroTPMPCR14	Filters access by the platform configuration register (PCR) 14 in the attestation document in the request. PCR14 is a contiguous measure of "MOK" certificates and hashes	String
kms:RecipientAttestation:NitroTPMPCR15	Filters access by the platform configuration register (PCR) 15 in the attestation document in the request. PCR15 is a contiguous measure of root file system volume encryption key	String
kms:RecipientAttestation:NitroTPMPCR16	Filters access by the platform configuration register (PCR) 16 in the attestation document in the request. PCR16 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR17	Filters access by the platform configuration register (PCR) 17 in the attestation document in the request. PCR17 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR18	Filters access by the platform configuration register (PCR) 18 in the attestation document in the request. PCR18 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR19	Filters access by the platform configuration register (PCR) 19 in the attestation document in the request. PCR19 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:NitroTPMPCR2	Filters access by the platform configuration register (PCR) 2 in the attestation document in the request. PCR2 is a contiguous measure of extended or pluggable executable code, including option ROMs on pluggable hardware	String
kms:RecipientAttestation:NitroTPMPCR20	Filters access by the platform configuration register (PCR) 20 in the attestation document in the request. PCR20 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR21	Filters access by the platform configuration register (PCR) 21 in the attestation document in the request. PCR21 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR22	Filters access by the platform configuration register (PCR) 22 in the attestation document in the request. PCR22 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR23	Filters access by the platform configuration register (PCR) 23 in the attestation document in the request. PCR23 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR3	Filters access by the platform configuration register (PCR) 3 in the attestation document in the request. PCR3 is a contiguous measure of extended or pluggable firmware data, including information about pluggable hardware	String

Condition keys	Description	Type
kms:RecipientAttestation:NitroTPMPCR4	Filters access by the platform configuration register (PCR) 4 in the attestation document in the request. PCR4 is a contiguous measure of boot loader and additional drivers, including binaries and extensions loaded by the boot loader	String
kms:RecipientAttestation:NitroTPMPCR5	Filters access by the platform configuration register (PCR) 5 in the attestation document in the request. PCR5 is a contiguous measure of GPT/Partition table	String
kms:RecipientAttestation:NitroTPMPCR6	Filters access by the platform configuration register (PCR) 6 in the attestation document in the request. PCR6 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR7	Filters access by the platform configuration register (PCR) 7 in the attestation document in the request. PCR7 is a contiguous measure of SecureBoot state	String
kms:RecipientAttestation:NitroTPMPCR8	Filters access by the platform configuration register (PCR) 8 in the attestation document in the request. PCR8 is a contiguous measure of commands and kernel command line	String
kms:RecipientAttestation:NitroTPMPCR9	Filters access by the platform configuration register (PCR) 9 in the attestation document in the request. PCR9 is a contiguous measure of all files read (including kernel image)	String
kms:RecipientAttestation:PCR0	Filters access by the platform configuration register (PCR) 0 in the attestation document in the request. PCR0 is a contiguous measure of the contents of the enclave image file, without the section data	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR1	Filters access by the platform configuration register (PCR) 1 in the attestation document in the request. PCR1 is a contiguous measurement of the Linux kernel and bootstrap data	String
kms:RecipientAttestation:PCR10	Filters access by the platform configuration register (PCR) 10 in the attestation document in the request. PCR10 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR11	Filters access by the platform configuration register (PCR) 11 in the attestation document in the request. PCR11 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR12	Filters access by the platform configuration register (PCR) 12 in the attestation document in the request. PCR12 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR13	Filters access by the platform configuration register (PCR) 13 in the attestation document in the request. PCR13 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR14	Filters access by the platform configuration register (PCR) 14 in the attestation document in the request. PCR14 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR15	Filters access by the platform configuration register (PCR) 15 in the attestation document in the request. PCR15 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR16	Filters access by the platform configuration register (PCR) 16 in the attestation document in the request. PCR16 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR17	Filters access by the platform configuration register (PCR) 17 in the attestation document in the request. PCR17 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR18	Filters access by the platform configuration register (PCR) 18 in the attestation document in the request. PCR18 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR19	Filters access by the platform configuration register (PCR) 19 in the attestation document in the request. PCR19 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR2	Filters access by the platform configuration register (PCR) 2 in the attestation document in the request. PCR2 is a contiguous, in-order measurement of the user applications, without the boot ramfs	String
kms:RecipientAttestation:PCR20	Filters access by the platform configuration register (PCR) 20 in the attestation document in the request. PCR20 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR21	Filters access by the platform configuration register (PCR) 21 in the attestation document in the request. PCR21 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR22	Filters access by the platform configuration register (PCR) 22 in the attestation document in the request. PCR22 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR23	Filters access by the platform configuration register (PCR) 23 in the attestation document in the request. PCR23 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR24	Filters access by the platform configuration register (PCR) 24 in the attestation document in the request. PCR24 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR25	Filters access by the platform configuration register (PCR) 25 in the attestation document in the request. PCR25 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR26	Filters access by the platform configuration register (PCR) 26 in the attestation document in the request. PCR26 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR27	Filters access by the platform configuration register (PCR) 27 in the attestation document in the request. PCR27 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR28	Filters access by the platform configuration register (PCR) 28 in the attestation document in the request. PCR28 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR29	Filters access by the platform configuration register (PCR) 29 in the attestation document in the request. PCR29 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR3	Filters access by the platform configuration register (PCR) 3 in the attestation document in the request. PCR3 is a contiguous measurement of the IAM role assigned to the parent instance	String
kms:RecipientAttestation:PCR30	Filters access by the platform configuration register (PCR) 30 in the attestation document in the request. PCR30 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR31	Filters access by the platform configuration register (PCR) 31 in the attestation document in the request. PCR31 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR4	Filters access by the platform configuration register (PCR) 4 in the attestation document in the request. PCR4 is a contiguous measurement of the ID of the parent instance	String
kms:RecipientAttestation:PCR5	Filters access by the platform configuration register (PCR) 5 in the attestation document in the request. PCR5 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR6	Filters access by the platform configuration register (PCR) 6 in the attestation document in the request. PCR6 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR7	Filters access by the platform configuration register (PCR) 7 in the attestation document in the request. PCR7 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR8	Filters access by the platform configuration register (PCR) 8 in the attestation document in the request. PCR8 is a measure of the signing certificate specified for the enclave image file	String
kms:RecipientAttestation:PCR9	Filters access by the platform configuration register (PCR) 9 in the attestation document in the request. PCR9 is a custom PCR that can be defined by the user for specific use cases	String
kms:ReplicaRegion	Filters access to the ReplicateKey operation based on the value of the ReplicaRegion parameter in the request	String
kms:RequestAlias	Filters access to cryptographic operations, DescribeKey, and GetPublicKey based on the alias in the request	String
kms:ResourceAliases	Filters access to specified AWS KMS operations based on aliases associated with the AWS KMS key	ArrayOfString
kms:RetiringPrincipal	Filters access to the CreateGrant operation based on the retiring principal in the grant	String
kms:RotationPeriodInDays	Filters access to the EnableKeyRotation operation based on the value of the RotationPeriodInDays parameter in the request	Numeric
kms:ScheduleKeyDeletionPendingWindowInDays	Filters access to the ScheduleKeyDeletion operation based on the value of the PendingWindowInDays parameter in the request	Numeric

Condition keys	Description	Type
kms:SigningAlgorithm	Filters access to the Sign and Verify operations based on the signing algorithm in the request	String
kms:ValidTo	Filters access to the ImportKeyMaterial operation based on the value of the ValidTo parameter in the request. You can use this condition key to allow users to import key material only when it expires by the specified date	Date
kms:ViaService	Filters access when a request made on the principal's behalf comes from a specified AWS service	String
kms:WrappingAlgorithm	Filters access to the GetParametersForImport operation based on the value of the WrappingAlgorithm parameter in the request	String
kms:WrappingKeySpec	Filters access to the GetParametersForImport operation based on the value of the WrappingKeySpec parameter in the request	String

Actions, resources, and condition keys for Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) (service prefix: `cassandra`) 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 Keyspaces (for Apache Cassandra)
- Resource types defined by Amazon Keyspaces (for Apache Cassandra)

- Condition keys for Amazon Keyspaces (for Apache Cassandra)

Actions defined by Amazon Keyspaces (for Apache Cassandra)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Alter	Grants permission to alter a keyspace or table	Write	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
AlterMultiRegionResource	Grants permission to alter a multiregion keyspace or table	Write	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Create	Grants permission to create a keyspace or table	Write	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMultiRegionResource	Grants permission to create a multiregion keyspace or table	Write	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
Drop	Grants permission to drop a keyspace or table	Write	keyspace		
			table		
DropMultiRegionResource	Grants permission to drop a multiregion keyspace or table	Write	keyspace		
			table		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRecords	Grants permission to retrieve the CDC stream records from a given shard	Read	stream*		
GetShardIterator	Grants permission to return a shard iterator	Read	stream*		
GetStream	Grants permission to return information about a CDC stream, including the composition of its shards	Read	stream*		
ListStreams	Grants permission to return an array of CDC stream ARNs associated with the current account and endpoint	List			
Modify	Grants permission to INSERT, UPDATE or DELETE data in a table	Write	table*		
ModifyMultiRegionResource	Grants permission to INSERT, UPDATE or DELETE data in a multiregion table	Write	table*		
Restore	Grants permission to restore table from a backup	Write	table*		
RestoreMultiRegionTable	Grants permission to restore multiregion table from a backup	Write	table*		
Select	Grants permission to SELECT data from a table	Read	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SelectMultiRegionResource	Grants permission to SELECT data from a multiregion table	Read	table*		
TagMultiRegionResource	Grants permission to tag a multiregion keyspace or table	Tagging	keyspace		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to tag a keyspace, table, or stream	Tagging	keyspace		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnTagMultiRegionResource	Grants permission to untag a multiregion keyspace or table	Tagging	keyspace		
			table		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UntagResource	Grants permission to untag a keyspace, table or stream	Tagging	keyspace		
			stream		
			table		
				aws:TagKeys	
UpdatePartitioner	Grants permission to UPDATE the partitioner in a system table	Write	table*		

Resource types defined by Amazon Keyspaces (for Apache Cassandra)

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
keyspace	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
stream	`arn:${Partition}:cassandra:${Region}:${Account}:/keyspace/${KeyspaceName}/table/${TableName}/stream/${StreamLabel}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddApplicationReferenceDataSource	Grants permission to add reference data source to the application	Write	application*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplicationCloudWatchLoggingOption	Grants permission to delete the specified cloudwatch logging option of the application	Write	application*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeApplicationOperation	Grants permission to describe an application operation of an application	Read	application*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RollbackApplication	Grants permission to perform rollback operation on an application	Write	application*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToStream	Grants permission to add or update tags for the specified Amazon Kinesis stream. Each stream can have up to 50 tags	Tagging	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	Grants permission to create a Amazon Kinesis stream	Write	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy	Grants permission to delete a resource policy associated with a specified stream or consumer	Write	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
DeleteStream	Grants permission to delete a stream and all its shards and data	Write	stream*	aws:ResourceTag/${TagKey}	
DeregisterStreamConsumer	Grants permission to deregister a stream consumer with a Kinesis data stream	Write	consumer*	aws:ResourceTag/${TagKey}	
DescribeAccountSettings	Grants permission to describe the account-level settings for Amazon Kinesis Data Streams	Read			
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStreamConsumer	Grants permission to get the description of a registered stream consumer	Read	consumer*	aws:ResourceTag/${TagKey}	
DescribeStreamSummary	Grants permission to provide a summarized description of the specified Kinesis data stream without the shard list	Read	stream*	aws:ResourceTag/${TagKey}	
DisableEnhancedMonitoring	Grants permission to disables enhanced monitoring	Write			
EnableEnhancedMonitoring	Grants permission to enable enhanced Kinesis data stream monitoring for shard-level metrics	Write			
GetRecords	Grants permission to get data records from a shard	Read	stream*	aws:ResourceTag/${TagKey}	
GetResourcePolicy	Grants permission to get a resource policy associated with a specified stream or consumer	Read	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetShardIterator	Grants permission to get a shard iterator. A shard iterator expires five minutes after it is returned to the requester	Read	stream*	aws:ResourceTag/${TagKey}	
IncreaseStreamRetentionPeriod	Grants permission to increase the stream's retention period, which is the length of time data records are accessible after they are added to the stream	Write	stream*	aws:ResourceTag/${TagKey}	
InjectApiError [permission only]	Grants permission to temporarily inject errors for target API requests	Write		kinesis:FisActionId kinesis:FisTargetArns kinesis:FisInjectPercentage	
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 AWS KMS key for a specified stream	Write	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopStreamEncryption	Grants permission to disable server-side encryption for a specified stream	Write	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	Grants permission to listen to a specific shard with enhanced fan-out	Read	consumer*	aws:ResourceTag/${TagKey}	
TagResource	Grants permission to add or update tags for the specified Amazon Kinesis resource. Each resource can have up to 50 tags	Tagging	consumer*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from the specified Kinesis data resource. Removed tags are deleted and cannot be recovered after this operation successfully completes	Tagging	consumer*	aws:TagKeys aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAccountSettings	Grants permission to update the account-level settings for Amazon Kinesis Data Streams	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMaxRecordSize	Grants permission to update the maximum record size for a Kinesis data stream	Write	stream*	aws:ResourceTag/${TagKey}	
UpdateShardCount	Grants permission to update the shard count of the specified stream to the specified number of shards	Write			
UpdateStreamMode	Grants permission to update the capacity mode of the data stream	Write			
UpdateStreamWarmThroughput	Grants permission to update the warm throughput for a Kinesis on-demand data stream	Write	stream*	aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Kinesis Data Streams

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
consumer	arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}	aws:ResourceTag/${TagKey}
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Condition keys for Amazon Kinesis Data Streams

Amazon Kinesis Data Streams defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
kinesis:FisActionId	Filters access by the ID of an AWS FIS action	String
kinesis:FisInjectPercentage	Filters access by the percentage of calls being affected by an AWS FIS action	Numeric

Condition keys	Description	Type
kinesis:FisTargetArns	Filters access by the ARN of an AWS FIS target	ArrayOfARN

Actions, resources, and condition keys for Amazon Kinesis Firehose

Amazon Kinesis Firehose (service prefix: `firehose`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Kinesis Firehose
- Resource types defined by Amazon Kinesis Firehose
- Condition keys for Amazon Kinesis Firehose

Actions defined by Amazon Kinesis Firehose

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDeliveryStream	Grants permission to create a delivery stream	Write	deliverystream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeliveryStream	Grants permission to delete a delivery stream and its data	Write	deliverystream*		
DescribeDeliveryStream	Grants permission to describe the specified delivery stream and gets the status	Read	deliverystream*		
ListDeliveryStreams	Grants permission to list your delivery streams	List			
ListTagsForDeliveryStream	Grants permission to list the tags for the specified delivery stream	List	deliverystream*		
PutRecord	Grants permission to write a single data record into an Amazon Kinesis Firehose delivery stream	Write	deliverystream*		
PutRecordBatch	Grants permission to write multiple data records into a delivery stream in a single call, which can achieve higher throughput per producer than when writing single records	Write	deliverystream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDeliveryStreamEncryption	Grants permission to enable server-side encryption (SSE) for the delivery stream	Write	deliverystream*		
StopDeliveryStreamEncryption	Grants permission to disable the specified destination of the specified delivery stream	Write	deliverystream*		
TagDeliveryStream	Grants permission to add or update tags for the specified delivery stream	Tagging	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	Grants permission to remove tags from the specified delivery stream	Tagging	deliverystream*		
				aws:TagKeys	
UpdateDestination	Grants permission to update the specified destination of the specified delivery stream	Write	deliverystream*		

Resource types defined by Amazon Kinesis Firehose

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types

that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Kinesis Firehose

Amazon Kinesis Firehose defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSignalingChannel	Grants permission to create a signaling channel	Write	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Grants permission to create a Kinesis video stream	Write	stream*		
				aws:RequestTag/${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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStreamStorageConfiguration	Grants permission to describe the stream storage configuration of your Kinesis Video Stream	Read	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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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		Read	channel		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to fetch the tags associated with your resource		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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from your resource	Tagging	channel		
			stream		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateStreamStorageConfiguration	Grants permission to update the stream storage configuration of your 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}

Resource types	ARN	Condition keys
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 AWS 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
aws:TagKeys	Filters requests based on the presence of mandatory tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Lake Formation

AWS Lake Formation (service prefix: lakeformation) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.

- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Lake Formation

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddLFTagsToResource	Grants permission to attach Lake Formation tags to catalog resources	Tagging			
BatchGrantPermissions	Grants permission to data lake permissions to one or more principals in a batch	Permissions management			
BatchRevokePermissions	Grants permission to revoke data lake permissions from one or more principals in a batch	Permissions management			
CancelTransaction	Grants permission to cancel the given transaction	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CommitTransaction	Grants permission to commit the given transaction	Write			
CreateDataCellsFilter	Grants permission to create a Lake Formation data cell filter	Write			
CreateLFTag	Grants permission to create a Lake Formation tag	Write			
CreateLFTagExpression	Grants permission to create a Lake Formation tag expression	Write			
CreateLakeFormationIdentityCenterConfiguration	Grants permission to create an IAM Identity Center connection with Lake Formation to allow IAM Identity Center users and groups to access Data Catalog resources	Write			
CreateLakeFormationOptIn	Grants permission to enforce Lake Formation permissions for the given databases, tables, and principals	Write			
DeleteDataCellsFilter	Grants permission to delete a Lake Formation data cell filter	Write			
DeleteLFTag	Grants permission to delete a Lake Formation tag	Write			
DeleteLFTagExpression	Grants permission to delete a Lake Formation expression	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLakeFormationIdentityCenterConfiguration	Grants permission to delete an IAM Identity Center connection with Lake Formation	Write			
DeleteLakeFormationOptIn	Grants permission to remove the Lake Formation permissions enforcement of the given databases, tables, and principals	Write			
DeleteObjectsOnCancel	Grants permission to delete the specified objects if the transaction is canceled	Write			
DeregisterResource	Grants permission to deregister a registered location	Write			
DescribeLakeFormationIdentityCenterConfiguration	Grants permission to describe the IAM Identity Center connection with Lake Formation	Read			
DescribeResource	Grants permission to describe a registered location	Read			
DescribeTransaction	Grants permission to get status of the given transaction	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExtendTransaction	Grants permission to extend the timeout of the given transaction	Write			
GetDataAccess	Grants permission to virtual data lake access	Write		lakeformation:EnabledOnlyForMetaDataAccess	
GetDataCellsFilter	Grants permission to retrieve a Lake Formation data cell filter	Read			
GetDataLakePrincipal	Grants permission to retrieve the identity of the invoking principal				
GetDataLakeSettings	Grants permission to retrieve data lake settings such as the list of data lake administrators and database and table default permissions	Read			
GetEffectivePermissionsForPath	Grants permission to retrieve permissions attached to resources in the given path	Read			
GetLFTag	Grants permission to retrieve a Lake Formation tag	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLFTagExpression	Grants permission to retrieve a Lake Formation tag expression	Read			
GetQueryState	Grants permission to retrieve the state of the given query	Read			lakeformation:StartQueryPlanning
GetQueryStatistics	Grants permission to retrieve the statistics for the given query	Read			lakeformation:StartQueryPlanning
GetResourceLFTags	Grants permission to retrieve lakeformation tags on a catalog resource	Read			
GetTableObjects	Grants permission to retrieve objects from a table	Read			
GetTemporaryGluePartitionCredentials	Grants permission to get temporary credentials to access Glue partition data through Lake Formation	Read			
GetTemporaryGlueTableCredentials	Grants permission to get temporary credentials to access Glue table data through Lake Formation	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWorkUnitResults	Grants permission to retrieve the results for the given work units	Read			lakeformation:GetWorkUnits lakeformation:StartQueryPlanning
GetWorkUnits	Grants permission to retrieve the work units for the given query	Read			lakeformation:StartQueryPlanning
GrantPermissions	Grants permission to data lake permissions to a principal	Permissions management			
ListDataCellsFilter	Grants permission to list cell filters	List			
ListLFTagExpressions	Grants permission to list Lake Foramtion tag expressions	Read			
ListLFTags	Grants permission to list Lake Formation tags	Read			
ListLakeFormationOptIns	Grants permission to retrieve the current list of resources and principals that are opt in to enforce Lake Formation permissions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPermissions	Grants permission to list permissions filtered by principal or resource	List			
ListResources	Grants permission to List registered locations	List			
ListTableStorageOptimizers	Grants permission to list all the storage optimizers for the Governed table	List			
ListTransactions	Grants permission to list all transactions in the system	List			
PutDataLakeSettings	Grants permission to overwrite data lake settings such as the list of data lake administrators and database and table default permissions	Permissions management			
RegisterResource	Grants permission to register a new location to be managed by Lake Formation	Write			
RegisterResourceWithPrivilegedAccess	Grants permission to register a new location to be managed by Lake Formation, with privileged access	Write			
RemoveLFTagsFromResource	Grants permission to remove lakeformation tags from catalog resources	Tagging			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokePermissions	Grants permission to revoke data lake permissions from a principal	Permissions management			
SearchDatabasesByLFTags	Grants permission to list catalog databases with Lake Formation tags	Read			
SearchTablesByLFTags	Grants permission to list catalog tables with Lake Formation tags	Read			
StartQueryPlanning	Grants permission to initiate the planning of the given query	Write			
StartTransaction	Grants permission to start a new transaction	Write			
UpdateDataCellsFilter	Grants permission to update a Lake Formation data cell filter	Write			
UpdateLFTag	Grants permission to update a Lake Formation tag	Write			
UpdateLFTagExpression	Grants permission to update a Lake Formation expression	Write			
UpdateLakeFormationIdentityCenterConfiguration	Grants permission to update the IAM Identity Center connection parameters	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResource	Grants permission to update a registered location	Write			
UpdateTableObjects	Grants permission to add or delete the specified objects to or from a table	Write			
UpdateTableStorageOptimizer	Grants permission to update the configuration of the storage optimizer for the Governed table	Write			

Resource types defined by AWS Lake Formation

AWS Lake Formation does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Lake Formation, specify `"Resource": "*"` in your policy.

Condition keys for AWS Lake Formation

AWS Lake Formation defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
lakeformation:Enab	Filters access by the presence of the key configured for role's identity-based policy	Bool

Condition keys	Description	Type
ledOnlyFo rMetaDataAccess		

Actions, resources, and condition keys for AWS Lambda

AWS Lambda (service prefix: `lambda`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Lambda
- Resource types defined by AWS Lambda
- Condition keys for AWS Lambda

Actions defined by AWS Lambda

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddLayerVersionPermission	Grants permission to add permissions to the resource-based policy of a version of an AWS Lambda layer	Permissions management	layerVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPermission	Grants permission to give an AWS service or another account permission to use an AWS Lambda function	Permissions management	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
CheckpointDurableExecution	Grants permission to save the progress of an AWS Lambda durable execution	Write	durable execution*		
CreateAlias	Grants permission to create an alias for a Lambda function version	Write	function*		
CreateCapacityProvider	Grants permission to create an AWS Lambda capacity provider	Write	capacityProvider*		iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys lambda:SecurityGroupIds lambda:SubnetIds	
CreateCodeSigningConfig	Grants permission to create an AWS Lambda code signing config	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	Grants permission to create a mapping between an event source and an AWS Lambda function	Write		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFunction	Grants permission to create an AWS Lambda function	Write	function*		iam:PassRole lambda:PassCapacityProvider
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFunctionUrlConfig	Grants permission to create a function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteAlias	Grants permission to delete an AWS Lambda function alias	Write	function*		
DeleteCapacityProvider	Grants permission to delete an AWS Lambda capacity provider	Write	capacityProvider*		
DeleteCodeSigningConfig	Grants permission to delete an AWS Lambda code signing config	Write	code signing config*		
DeleteEventSourceMapping	Grants permission to delete an AWS Lambda event source mapping	Write	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Grants permission to delete an AWS Lambda function	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFunctionCodeSigningConfig	Grants permission to detach a code signing config from an AWS Lambda function	Write	function*		
DeleteFunctionConcurrency	Grants permission to remove a concurrent execution limit from an AWS Lambda function	Write	function*		
DeleteFunctionEventInvokeConfig	Grants permission to delete the configuration for asynchronous invocation for an AWS Lambda function, version, or alias	Write	function*		
DeleteFunctionUrlConfig	Grants permission to delete function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	Grants permission to delete a version of an AWS Lambda layer	Write	layerVersion*		
DeleteProvisionedConcurrencyConfig	Grants permission to delete the provisioned concurrency configuration for an AWS Lambda function	Write	function alias		
			function version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Region	Read			
GetAlias	Grants permission to view details about an AWS Lambda function alias	Read	function*		
GetCapacityProvider	Grants permission to view details about an AWS Lambda capacity provider	Read	capacityProvider*		
GetCodeSigningConfig	Grants permission to view details about an AWS Lambda code signing config	Read	code signing config*		
GetDurableExecution	Grants permission to view details of an AWS Lambda durable execution	Read	durable execution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDurableExecutionHistory	Grants permission to view execution history of an AWS Lambda durable execution	Read	durable execution*		
GetDurableExecutionState	Grants permission to view current state of an AWS Lambda durable execution	Read	durable execution*		
GetEventSourceMapping	Grants permission to view details about an AWS Lambda event source mapping	Read	eventSourceMapping*		
				lambda:FunctionArn	
GetFunction	Grants permission to view details about an AWS Lambda function	Read	function*		
GetFunctionCodeSigningConfig	Grants permission to view the code signing config arn attached to an AWS Lambda function	Read	function*		
GetFunctionConcurrency	Grants permission to view details about the reserved concurrency configuration for a function	Read	function*		
GetFunctionConfiguration	Grants permission to view details about the version-specific settings of an AWS Lambda function or version	Read	function*		

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 AWS Lambda function	Read	function*		
GetFunctionScalingConfig	Grants permission to view the scaling configuration of an AWS Lambda function running on a capacity provider	Read	function*		
GetFunctionUrlConfig	Grants permission to read function url configuration for a Lambda function	Read	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
GetLayerVersion	Grants permission to view details about a version of an AWS Lambda layer. Note this action also supports GetLayerVersionByArn API	Read	layerVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLayerVersionPolicy	Grants permission to view the resource-based policy for a version of an AWS Lambda layer	Read	layerVersion*		
GetPolicy	Grants permission to view the resource-based policy for an AWS Lambda function, version, or alias	Read	function*		
GetProvisionedConcurrencyConfig	Grants permission to view the provisioned concurrency configuration for an AWS Lambda function's alias or version	Read	function alias		
			function version		
GetRuntimeManagementConfig	Grants permission to view the runtime management configuration of an AWS Lambda function	Read	function*		
InvokeAsync	Grants permission to invoke a function asynchronously (Deprecated)	Write	function*		
InvokeFunction	Grants permission to invoke an AWS Lambda function	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:EventSourceToken lambda:InvokedViaFunctionUrl	
InvokeFunctionUrl [permission only]	Grants permission to invoke an AWS Lambda function through url	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	Grants permission to retrieve a list of aliases for an AWS Lambda function	List	function*		
ListCapacityProviders	Grants permission to retrieve a list of AWS Lambda capacity providers	List			
ListCodeSigningConfigs	Grants permission to retrieve a list of AWS Lambda code signing configs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDurableExecutionsByFunction	Grants permission to retrieve a list of AWS Lambda durable executions of an AWS Lambda function	List	function*		
ListEventSourceMappings	Grants permission to retrieve a list of AWS Lambda event source mappings	List			
ListFunctionEventInvokeConfigs	Grants permission to retrieve a list of configurations for asynchronous invocation for a function	List	function*		
ListFunctionUrlConfigs	Grants permission to read function url configurations for a function	List	function*		
				lambda:FunctionUrlAuthType	
ListFunctionVersionsByCapacityProvider	Grants permission to retrieve a list of AWS Lambda function versions by the capacity provider assigned	List	capacityProvider*		
ListFunctions	Grants permission to retrieve a list of AWS Lambda functions, with the version-specific configuration of each function	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFunctionsByCodeSigningConfig	Grants permission to retrieve a list of AWS Lambda functions by the code signing config assigned	List	code signing config*		
ListLayerVersions	Grants permission to retrieve a list of versions of an AWS Lambda layer	List			
ListLayers	Grants permission to retrieve a list of AWS Lambda layers, with details about the latest version of each layer	List			
ListProvisionedConcurrencyConfigs	Grants permission to retrieve a list of provisioned concurrency configurations for an AWS Lambda function	List	function*		
ListTags	Grants permission to retrieve a list of tags for an AWS Lambda function, event source mapping, capacity provider, or code signing configuration resource	Read	capacityProvider		
			code signing config		
			eventSourceMapping		
			function		
ListVersionsByFunction	Grants permission to retrieve a list of versions for an AWS Lambda function	List	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PassCapacityProvider [permission only]	Grants permission to pass an AWS Lambda capacity provider to a service	Write	capacityProvider*		
PublishLayerVersion	Grants permission to create an AWS Lambda layer	Write	layer*		
PublishVersion	Grants permission to create an AWS Lambda function version	Write	function*		
PutFunctionCodeSigningConfig	Grants permission to attach a code signing config to an AWS Lambda function	Write	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Grants permission to configure reserved concurrency for an AWS Lambda function	Write	function*		
PutFunctionEventInvokeConfig	Grants permission to configures options for asynchronous invocation on an AWS Lambda function, version, or alias	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFunctionRecursionConfig	Grants permission to update the recursion configuration of an AWS Lambda function	Write	function*		
PutFunctionScalingConfig	Grants permission to update the scaling configuration of an AWS Lambda function running on a capacity provider	Write	function*		
PutProvisionedConcurrencyConfig	Grants permission to configure provisioned concurrency for an AWS Lambda function's alias or version	Write	function alias		
			function version		
PutRuntimeManagementConfig	Grants permission to update the runtime management configuration of an AWS Lambda function	Write	function*		
RemoveLayerVersionPermission	Grants permission to remove a statement from the permissions policy for a version of an AWS Lambda layer	Permissions management	layerVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemovePermission	Grants permission to revoke function-use permission from an AWS service or another account	Permissions management	function*		
				lambda:PrincipalLambda:FunctionUrlAuthType	
SendDurableExecutionCallbackFailure	Grants permission to send a failure response for a callback operation in an AWS Lambda durable execution	Write	durable execution*		
SendDurableExecutionCallbackHeartbeat	Grants permission to send a heartbeat for a callback operation in an AWS Lambda durable execution	Write	durable execution*		
SendDurableExecutionCallbackSuccess	Grants permission to send a successful response for a callback operation in an AWS Lambda durable execution	Write	durable execution*		
StopDurableExecution	Grants permission to stop an AWS Lambda durable execution	Write	durable execution*		
TagResource	Grants permission to add tags to an AWS Lambda function, event source mapping, capacity provider, or code signing configuration resource	Tagging	capacityProvider		
			code signing config		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			eventSourceMapping		
			function		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from an AWS Lambda function, event source mapping, capacity provider, or code signing configuration resource	Tagging	capacityProvider		
			code signing config		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	Grants permission to update the configuration of an AWS Lambda function's alias	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCapacityProvider	Grants permission to update an AWS Lambda capacity provider	Write	capacityProvider*		
UpdateCodeSigningConfig	Grants permission to update an AWS Lambda code signing config	Write	codesigningconfig*		
UpdateEventSourceMapping	Grants permission to update the configuration of an AWS Lambda event source mapping	Write	eventSourceMapping*		
				lambda:FunctionArn	
UpdateFunctionCode	Grants permission to update the code of an AWS Lambda function	Write	function*		
UpdateFunctionCodeSigningConfig	Grants permission to update the code signing config of an AWS Lambda function	Write	codesigningconfig*		
			function*		
UpdateFunctionConfiguration	Grants permission to modify the version-specific settings of an AWS Lambda function	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	Grants permission to modify the configuration for asynchronous invocation for an AWS Lambda function, version, or alias	Write	function*		
UpdateFunctionUrlConfig	Grants permission to update a function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Resource types defined by AWS Lambda

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
capacityProvider	arn:${Partition}:lambda:${Region}:${Account}:capacity-provider:${CapacityProviderName}	aws:ResourceTag/${TagKey}
code signing config	arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}	aws:ResourceTag/${TagKey}
durable execution	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}/durable-execution/${ExecutionName}/${ExecutionId}	
eventSourceMapping	arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}	aws:ResourceTag/${TagKey}
function	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}	aws:ResourceTag/${TagKey}
function alias	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}	aws:ResourceTag/${TagKey}
function version	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}	aws:ResourceTag/${TagKey}
layer	arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}	

Resource types	ARN	Condition keys
layerVersion	`arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}`	

Condition keys for AWS Lambda

AWS Lambda defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
lambda:CodeSigningConfigArn	Filters access by the ARN of an AWS Lambda code signing config	ARN
lambda:EventSourceToken	Filters access by the ID from a non-AWS event source configured for the AWS Lambda function	String
lambda:FunctionArn	Filters access by the ARN of an AWS Lambda function	ARN

Condition keys	Description	Type
lambda:FunctionUrlAuthType	Filters access by authorization type specified in request. Available during CreateFunctionUrlConfig, UpdateFunctionUrlConfig, DeleteFunctionUrlConfig, GetFunctionUrlConfig, ListFunctionUrlConfig, AddPermission and RemovePermission operations	String
lambda:InvokedViaFunctionUrl	Limits the scope of lambda:InvokeFunction action to Function URLs only. Available during AddPermission operation	Bool
lambda:Layer	Filters access by the ARN of a version of an AWS Lambda layer	ArrayOfString
lambda:Principal	Filters access by restricting the AWS service or account that can invoke a function	String
lambda:SecurityGroupIds	Filters access by the ID of security groups configured for the AWS Lambda function	ArrayOfString
lambda:SourceFunctionArn	Filters access by the ARN of the AWS Lambda function from which the request originated	ARN
lambda:SubnetIds	Filters access by the ID of subnets configured for the AWS Lambda function	ArrayOfString
lambda:VpcIds	Filters access by the ID of the VPC configured for the AWS Lambda function	String

Actions, resources, and condition keys for AWS Launch Wizard

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 [permission only]	Grants permission to create an application settings set	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
GetDeploymentPatternVersion	Grants permission to get a version of a deployment pattern	Read			
GetInfrastructureSuggestion [permission only]	Grants permission to get infrastructure suggestion	Read			
GetIpAddress [permission only]	Grants permission to get customer's ip address	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourceCostEstimate [permission only]	Grants permission to get resource cost estimate	Read			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAdditionalNodes [permission only]	Grants permission to list additional nodes	List			
ListAllowedResources [permission only]	Grants permission to list the allowed resources	List			
ListDeploymentEvents	Grants permission to list the events that occured during a deployment	List			
ListDeploymentPatternVersions	Grants permission to list the versions of a deployment pattern	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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	
UpdateDeployment	Grants permission to update a deployment	Write	deployment*	aws:ResourceTag/${TagKey}	
UpdateSettingsSet [permission only]	Grants permission to update an application settings set	Write			

Resource types defined by AWS 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 AWS Launch Wizard

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Lex

Amazon Lex (service prefix: `lex`) 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 Lex

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBotVersion	Creates a new version based on the $LATEST version of the specified bot	Write	bot version*		
CreateIntentVersion	Creates a new version based on the $LATEST version of the specified intent	Write	intent version*		
CreateSlotTypeVersion	Creates a new version based on the $LATEST version of the specified slot type	Write	slottype version*		
DeleteBot	Deletes all versions of a bot	Write	bot version*		
DeleteBotAlias	Deletes an alias for a specific bot	Write	bot alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBotChannelAssociation	Deletes the association between a Amazon Lex bot alias and a messaging platform	Write	channel*		
DeleteBotVersion	Deletes a specific version of a bot	Write	bot version*		
DeleteIntent	Deletes all versions of an intent	Write	intent version*		
DeleteIntentVersion	Deletes a specific version of an intent	Write	intent version*		
DeleteSession	Removes session information for a specified bot, alias, and user ID	Write	bot alias		
			bot version		
DeleteSlotType	Deletes all versions of a slot type	Write	slottype version*		
DeleteSlotTypeVersion	Deletes a specific version of a slot type	Write	slottype version*		
DeleteUtterances	Deletes the information Amazon Lex maintains for utterances on a specific bot and userId	Write	bot version*		
GetBot	Returns information for a specific bot. In addition to the bot name, the bot version or alias is required	Read	bot alias		
			bot version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBotAlias	Returns information about a Amazon Lex bot alias	Read	bot alias*		
GetBotAliases	Returns a list of aliases for a given Amazon Lex bot	List			
GetBotChannelAssociation	Returns information about the association between a Amazon Lex bot and a messaging platform	Read	channel*		
GetBotChannelAssociations	Returns a list of all of the channels associated with a single bot	List	channel*		
GetBotVersions	Returns information for all versions of a specific bot	List	bot version*		
GetBots	Returns information for the $LATEST version of all bots, subject to filters provided by the client	List			
GetBuiltinIntent	Returns information about a built-in intent	Read			
GetBuiltinIntents	Gets a list of built-in intents that meet the specified criteria	Read			
GetBuiltinSlotTypes	Gets a list of built-in slot types that meet the specified criteria	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExport	Exports Amazon Lex Resource in a requested format	Read	bot version*		
GetImport	Gets information about an import job started with StartImport	Read			
GetIntent	Returns information for a specific intent. In addition to the intent name, you must also specify the intent version	Read	intent version*		
GetIntentVersions	Returns information for all versions of a specific intent	List	intent version*		
GetIntents	Returns information for the $LATEST version of all intents, subject to filters provided by the client	List			
GetMigration	Grants permission to view an ongoing or completed migration	Read			
GetMigrations	Grants permission to view list of migrations from Amazon Lex v1 to Amazon Lex v2	List			
GetSession	Returns session information for a specified bot, alias, and user ID	Read	bot alias		
			bot version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSlotType	Returns information about a specific version of a slot type. In addition to specifying the slot type name, you must also specify the slot type version	Read	slottype version*		
GetSlotTypeVersions	Returns information for all versions of a specific slot type	List	slottype version*		
GetSlotTypes	Returns information for the $LATEST version of all slot types, subject to filters provided by the client	List			
GetUtterancesView	Returns a view of aggregate utterance data for versions of a bot for a recent time period	List	bot version*		
ListTagsForResource	Lists tags for a Lex resource	Read	bot		
			bot alias		
			channel		
PostContent	Sends user input (text or speech) to Amazon Lex	Write	bot alias		
			bot version		
PostText	Sends user input (text-only) to Amazon Lex	Write	bot alias		
			bot version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBot	Creates or updates the $LATEST version of a Amazon Lex conversational bot	Write	bot version*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutBotAlias	Creates or updates an alias for the specific bot	Write	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
PutIntent	Creates or updates the $LATEST version of an intent	Write	intent version*		
PutSession	Creates a new session or modifies an existing session with an Amazon Lex bot	Write	bot alias		
			bot version		
PutSlotType	Creates or updates the $LATEST version of a slot type	Write	slottype version*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartImport	Starts a job to import a resource to Amazon Lex	Write			
StartMigration	Grants permission to migrate a bot from Amazon Lex v1 to Amazon Lex v2	Write	bot version*		
TagResource	Adds or overwrites tags to a Lex resource	Tagging	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Removes tags from a Lex resource	Tagging	bot		
			bot alias		
			channel		
				aws:TagKeys aws:RequestTag/${TagKey}	

Resource types defined by Amazon Lex

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
bot	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}`	aws:ResourceTag/${TagKey}
bot version	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotVersion}`	aws:ResourceTag/${TagKey}
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot:${BotName}:${BotAlias}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:lex:${Region}:${Account}:bot-channel:${BotName}:${BotAlias}:${ChannelName}`	aws:ResourceTag/${TagKey}
intent version	`arn:${Partition}:lex:${Region}:${Account}:intent:${IntentName}:${IntentVersion}`	
slottype version	`arn:${Partition}:lex:${Region}:${Account}:slottype:${SlotName}:${SlotVersion}`	

Condition keys for Amazon Lex

Amazon Lex defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to a Lex resource	String
aws:TagKeys	Filters access based on the set of tag keys in the request	ArrayOfString
lex:associatedIntents	Enables you to control access based on the intents included in the request	ArrayOfString
lex:associatedSlotTypes	Enables you to control access based on the slot types included in the request	ArrayOfString
lex:channelType	Enables you to control access based on the channel type included in the request	String

Actions, resources, and condition keys for Amazon Lex V2

Amazon Lex V2 (service prefix: `lex`) 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 Lex V2
- Resource types defined by Amazon Lex V2

- Condition keys for Amazon Lex V2

Actions defined by Amazon Lex V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateCustomVocabularyItem	Grants permission to create new items in an existing custom vocabulary	Write	bot*		
BatchDeleteCustomVocabularyItem	Grants permission to delete existing items in an existing custom vocabulary	Write	bot*		
BatchUpdateCustomVocabularyItem	Grants permission to update existing items in an existing custom vocabulary	Write	bot*		
BuildBotLocale	Grants permission to build an existing bot locale in a bot	Write	bot*		
CreateBot	Grants permission to create a new bot and a test bot alias pointing to the DRAFT bot version	Write	bot*		
			bot alias*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
CreateBotAlias	Grants permission to create a new bot alias in a bot	Write	bot alias*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateBotChannel [permission only]	Grants permission to create a bot channel in an existing bot	Write	bot*		
CreateBotLocale	Grants permission to create a new bot locale in an existing bot	Write	bot*		
CreateBotReplica	Grants permission to create bot replica for a bot	Write	bot*		
CreateBotVersion	Grants permission to create a new version of an existing bot	Write	bot*		
CreateCustomVocabulary [permission only]	Grants permission to create a new custom vocabulary in an existing bot locale	Write	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExport	Grants permission to create an export for an existing resource	Write	bot		
			test set		
CreateIntent	Grants permission to create a new intent in an existing bot locale	Write	bot*		
CreateResourcePolicy	Grants permission to create a new resource policy for a Lex resource	Write	bot		
			bot alias		
CreateResourcePolicyStatement	Grants permission to create a new resource policy statement for a Lex resource	Write	bot		
			bot alias		
CreateSlot	Grants permission to create a new slot in an intent	Write	bot*		
CreateSlotType	Grants permission to create a new slot type in an existing bot locale	Write	bot*		
CreateTestSet [permission only]	Grants permission to import a new test-set	Write			
CreateTestSetDiscrepancyReport	Grants permission to create a test set discrepancy report	Write	test set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUploadUrl	Grants permission to create an upload url for import file	Write			
DeleteBot	Grants permission to delete an existing bot	Write	bot*		lex:DeleteBotAlias lex:DeleteBotChannel lex:DeleteBotLocale lex:DeleteBotVersion lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
			bot alias*		
DeleteBotAlias	Grants permission to delete an existing bot alias in a bot	Write	bot alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBotAnalyzerRecommendation	Grants permission to delete a bot analyzer recommendation	Write	bot*		
DeleteBotChannel [permission only]	Grants permission to delete an existing bot channel	Write	bot*		
DeleteBotLocale	Grants permission to delete an existing bot locale in a bot	Write	bot*		lex:DeleteIntent lex:DeleteSlot lex:DeleteSlotType
DeleteBotReplica	Grants permission to delete an existing bot replica	Write	bot*		
DeleteBotVersion	Grants permission to delete an existing bot version	Write	bot*		
DeleteCustomVocabulary	Grants permission to delete an existing custom vocabulary in a bot locale	Write	bot*		
DeleteExport	Grants permission to delete an existing export	Write	bot		
			test set		
DeleteImport	Grants permission to delete an existing import	Write	bot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			test set		
DeleteIntent	Grants permission to delete an existing intent in a bot locale	Write	bot*		
DeleteResourcePolicy	Grants permission to delete an existing resource policy for a Lex resource	Write	bot		
			bot alias		
DeleteResourcePolicyStatement	Grants permission to delete an existing resource policy statement for a Lex resource	Write	bot		
			bot alias		
DeleteSession	Grants permission to delete session information for a bot alias and user ID	Write	bot alias*		
DeleteSlot	Grants permission to delete an existing slot in an intent	Write	bot*		
DeleteSlotType	Grants permission to delete an existing slot type in a bot locale	Write	bot*		
DeleteTestSet	Grants permission to delete an existing test set	Write	test set*		
DeleteUtterances	Grants permission to delete utterance data for a bot	Write	bot*		
DescribeBot	Grants permission to retrieve an existing bot	Read	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBotAlias	Grants permission to retrieve an existing bot alias	Read	bot alias*		
DescribeBotAnalyzerRecommendation	Grants permission to describe a bot analyzer recommendation	Read	bot*		
DescribeBotChannel [permission only]	Grants permission to retrieve an existing bot channel	Read	bot*		
DescribeBotLocale	Grants permission to retrieve an existing bot locale	Read	bot*		
DescribeBotRecommendation	Grants permission to retrieve metadata information about a bot recommendation	Read	bot*		
DescribeBotReplica	Grants permission to retrieve an existing bot replica	Read	bot*		
DescribeBotResourceGeneration	Grants permission to retrieve metadata information for a bot resource generation	Read	bot*		
DescribeBotVersion	Grants permission to retrieve an existing bot version	Read	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCustomVocabulary [permission only]	Grants permission to retrieve an existing custom vocabulary	Read	bot*		
DescribeCustomVocabularyMetadata	Grants permission to retrieve metadata of an existing custom vocabulary	Read	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeExport	Grants permission to retrieve an existing export	Read	bot		lex:DescribeBot lex:DescribeBotLocale lex:DescribeIntent lex:DescribeSlot lex:DescribeSlotType lex:ListBotLocales lex:ListIntents lex:ListSlotTypes lex:ListSlots
			test set		
DescribeImport	Grants permission to retrieve an existing import	Read	bot		
			test set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIntent	Grants permission to retrieve an existing intent	Read	bot*		
DescribeResourcePolicy	Grants permission to retrieve an existing resource policy for a Lex resource	Read	bot		
			bot alias		
DescribeSlot	Grants permission to retrieve an existing slot	Read	bot*		
DescribeSlotType	Grants permission to retrieve an existing slot type	Read	bot*		
DescribeTestExecution	Grants permission to retrieve test execution metadata	Read	test set*		
DescribeTestSet	Grants permission to retrieve an existing test set	Read	test set*		
DescribeTestSetDiscrepancyReport	Grants permission to retrieve test set discrepancy report metadata	Read	test set*		
DescribeTestSetGeneration	Grants permission to retrieve test set generation metadata	Read	test set		
GenerateBotElement	Grants permission to generate supported fields or elements for a bot	Read	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSession	Grants permission to retrieve session information for a bot alias and user ID	Read	bot alias*		
GetTestExecutionArtifactsUrl	Grants permission to retrieve artifacts URL for a test execution	Read	test set*		
ListAggregatedUtterances	Grants permission to list utterances and statistics for a bot	List	bot*		
ListBotAliasReplicas	Grants permission to list alias replicas in a bot replica	List	bot*		
ListBotAliases	Grants permission to list bot aliases in an bot	List	bot*		
ListBotAnalyzerRecommendations	Grants permission to list bot analyzer recommendations	List	bot*		
ListBotChannels [permission only]	Grants permission to list bot channels	List	bot*		
ListBotLocales	Grants permission to list bot locales in a bot	List	bot*		
ListBotRecommendations	Grants permission to get a list of bot recommendations that meet the specified criteria	List	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBotReplicas	Grants permission to list replicas of a bot	List	bot*		
ListBotResourceGenerations	Grants permission to list the resource generations for a bot	List	bot*		
ListBotVersionReplicas	Grants permission to list version replicas in a bot replica	List	bot*		
ListBotVersions	Grants permission to list existing bot versions	List	bot*		
ListBots	Grants permission to list existing bots	List			
ListBuiltInIntents	Grants permission to list built-in intents	List			
ListBuiltInSlotTypes	Grants permission to list built-in slot types	List			
ListCustomVocabularyItems	Grants permission to list items of an existing custom vocabulary	List	bot*		
ListExports	Grants permission to list existing exports	List			
ListImports	Grants permission to list existing imports	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIntentMetrics	Grants permission to list intent analytics metrics for a bot	List	bot*		
ListIntentPaths	Grants permission to list intent path analytics for a bot	List	bot*		
ListIntentStageMetrics	Grants permission to list intentStage analytics metrics for a bot	List	bot*		
ListIntents	Grants permission to list intents in a bot	List	bot*		
ListRecommendedIntents	Grants permission to get a list of recommended intents provided by the bot recommendation	List	bot*		
ListSessionAnalyticsData	Grants permission to list session analytics data for a bot	List	bot*		
ListSessionMetrics	Grants permission to list session analytics metrics for a bot	List	bot*		
ListSlotTypes	Grants permission to list slot types in a bot	List	bot*		
ListSlots	Grants permission to list slots in an intent	List	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to lists tags for a Lex resource	Read	bot		
			bot alias		
			test set		
ListTestExecutionResultItems	Grants permission to retrieve test results data for a test execution	Read	test set*		lex:ListTestSetRecords
ListTestExecutions	Grants permission to list test executions	List			
ListTestSetRecords	Grants permission to retrieve records inside an existing test set	Read	test set*		
ListTestSets	Grants permission to list test sets	List			
PutSession	Grants permission to create a new session or modify an existing session for a bot alias and user ID	Write	bot alias*		
RecognizeText	Grants permission to send user input (text-only) to an bot alias	Write	bot alias*		
RecognizeUtterance	Grants permission to send user input (text or speech) to an bot alias	Write	bot alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchAssociatedTranscripts	Grants permission to search for associated transcripts that meet the specified criteria	List	bot*		
StartBotAnalyzer	Grants permission to start a bot analyzer for an existing bot locale	Write	bot*		
StartBotRecommendation	Grants permission to start a bot recommendation for an existing bot locale	Write	bot*		
StartBotResourceGeneration	Grants permission to start a resource generation for an existing bot locale	Write	bot*		
StartConversation	Grants permission to stream user input (speech/text/DTMF) to a bot alias	Write	bot alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartImport	Grants permission to start a new import with the uploaded import file	Write	bot		lex:CreateBot lex:CreateBotLocale lex:CreateCustomVocabulary lex:CreateIntent lex:CreateSlot lex:CreateSlotType lex:CreateTestSet lex:DeleteBotLocale lex:DeleteCustomVocabulary lex:DeleteIntent

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					lex:DeleteSlot lex:DeleteSlotType lex:UpdateBot lex:UpdateBotLocale lex:UpdateCustomVocabulary lex:UpdateIntent lex:UpdateSlot lex:UpdateSlotType lex:UpdateTestSet
			bot alias		
			test set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
StartTestExecution	Grants permission to start a test execution using a test set	Write	test set*		
StartTestSetGeneration	Grants permission to generate a test set	Write	test set		
StopBotAnalyzer	Grants permission to stop a bot analyzer for an existing bot locale	Write	bot*		
StopBotRecommendation	Grants permission to stop a bot recommendation for an existing bot locale	Write	bot*		
TagResource	Grants permission to add or overwrite tags of a Lex resource	Tagging	bot		
			bot alias		
			test set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a Lex resource	Tagging	bot		
			bot alias		
			test set		
				aws:TagKeys	
UpdateBot	Grants permission to update an existing bot	Write	bot*		
UpdateBotAlias	Grants permission to update an existing bot alias	Write	bot alias*		
UpdateBotLocale	Grants permission to update an existing bot locale	Write	bot*		
UpdateBotRecommendation	Grants permission to update an existing bot recommendation request	Write	bot*		
UpdateCustomVocabulary [permission only]	Grants permission to update an existing custom vocabulary	Write	bot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExport	Grants permission to update an existing export	Write	bot*		
UpdateIntent	Grants permission to update an existing intent	Write	bot*		
UpdateResourcePolicy	Grants permission to update an existing resource policy for a Lex resource	Write	bot		
			bot alias		
UpdateSlot	Grants permission to update an existing slot	Write	bot*		
UpdateSlotType	Grants permission to update an existing slot type	Write	bot*		
UpdateTestSet	Grants permission to update an existing test set	Write	test set*		

Resource types defined by Amazon Lex 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
bot	`arn:${Partition}:lex:${Region}:${Account}:bot/${BotId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
bot alias	`arn:${Partition}:lex:${Region}:${Account}:bot-alias/${BotId}/${BotAliasId}`	aws:ResourceTag/${TagKey}
test set	`arn:${Partition}:lex:${Region}:${Account}:test-set/${TestSetId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Lex V2

Amazon Lex V2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to a Lex resource	String
aws:TagKeys	Filters access by the set of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS License Manager

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateGrantVersion	Grants permission to create new version of grant	Write	grant*		
CreateLicense	Grants permission to create a new license	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseAssetGroup	Grants permission to create a license asset group	Write	license-asset-ruleset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLicenseAssetRuleset	Grants permission to create a license asset ruleset	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 supported license manager resources	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	Grants permission to create new version of license	Write	license*		
CreateToken	Grants permission to create a new token for license	Write	license*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGrant	Grants permission to delete a grant	Write	grant*		
DeleteLicense	Grants permission to delete a license	Write	license*		
DeleteLicenseAssetGroup	Grants permission to delete a license asset group	Write	license-asset-group*		
DeleteLicenseAssetRuleset	Grants permission to delete a license asset ruleset	Write	license-asset-ruleset*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGrant	Grants permission to get a grant	Read	grant*		
GetLicense	Grants permission to get a license	Read	license*		
GetLicenseAssetGroup	Grants permission to get a license asset group	Read	license-asset-group*		
GetLicenseAssetRuleset	Grants permission to get a license asset ruleset	Read	license-asset-ruleset*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssetsForLicenseAssetGroup	Grants permission to list assets for a license asset group	List	license-asset-group*		
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*		
ListLicenseAssetGroups	Grants permission to list license asset groups	List	license-asset-group		
ListLicenseAssetRulesets	Grants permission to list license asset rulesets	List	license-asset-ruleset		
ListLicenseConfigurations	Grants permission to list license configurations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLicenseConfigurationsForOrganization	Grants permission to list license configurations for organization	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListReceivedLicenses	Grants permission to list received licenses	List			
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-asset-group		
			license-asset-ruleset		
			license-configuration		
			report-generator		
ListTokens	Grants permission to list tokens	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			license-asset-group		
			license-asset-ruleset		
			license-configuration		
			report-generator		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a selected resource	Tagging	grant		
			license		
			license-asset-group		
			license-asset-ruleset		
			license-configuration		
			report-generator		
				aws:TagKeys	
UpdateLicenseAssetGroup	Grants permission to update a license asset group	Write	license-asset-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			license-asset-ruleset*		
UpdateLicenseAssetRuleset	Grants permission to update a license asset ruleset	Write	license-asset-ruleset*		
UpdateLicenseConfiguration	Grants permission to update an existing license configuration	Write	license-configuration*		
UpdateLicenseManagerReportGenerator	Grants permission to update a report generator for supported license manager resources	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 AWS 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}
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}
license-asset-ruleset	arn:${Partition}:license-manager:${Region}:${Account}:license-asset-ruleset:${LicenseAssetRulesetId}	aws:ResourceTag/${TagKey}
license-asset-group	arn:${Partition}:license-manager:${Region}:${Account}:license-asset-group:${LicenseAssetGroupId}	aws:ResourceTag/${TagKey}

Condition keys for AWS License Manager

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString
license-manager:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String

Actions, resources, and condition keys for AWS License Manager Linux Subscriptions Manager

AWS 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 AWS License Manager Linux Subscriptions Manager
- Resource types defined by AWS License Manager Linux Subscriptions Manager
- Condition keys for AWS License Manager Linux Subscriptions Manager

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterSubscriptionProvider	Grants permission to permanently delete a subscription provider in AWS License Manager	Write	subscription-provider*		
GetRegisteredSubscriptionProvider	Grants permission to get a subscription provider in AWS License Manager	Read	subscription-provider*		
GetServiceSettings	Grants permission to get the service settings for Linux subscriptions in AWS License Manager	Read			
ListLinuxSubscriptionInstances	Grants permission to list all instances with Linux subscriptions in AWS License Manager	Read			
ListLinuxSubscriptions	Grants permission to list all Linux subscriptions in AWS License Manager	Read			
ListRegisteredSubscriptionProviders	Grants permission to list subscription providers in AWS License Manager	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a selected resource	Read	subscription-provider*		
RegisterSubscriptionProvider	Grants permission to create a new subscription provider in AWS License Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to tag a selected resource	Tagging	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a selected resource	Tagging	subscription-provider*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceSettings	Grants permission to update the service settings for Linux subscriptions in AWS License Manager	Write			

Resource types defined by AWS 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 AWS License Manager Linux Subscriptions Manager

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 AWS License Manager User Subscriptions

AWS License Manager User Subscriptions (service prefix: `license-manager-user-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 AWS License Manager User Subscriptions
- Resource types defined by AWS License Manager User Subscriptions
- Condition keys for AWS License Manager User Subscriptions

Actions defined by AWS License Manager User Subscriptions

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateUser	Grants permission to associate a subscribed user to an instance launched with license manager user subscriptions products	Write	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseServerEndpoint	Grants permission to create a license server endpoint for a given server type for a given Identity Provider	Write	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLicenseServerEndpoint	Grants permission to delete a license server endpoint for a given server type for a given Identity Provider	Write	identity-provider*		
			license-server-endpoint*		
DeregisterIdentityProvider	Grants permission to deregister Microsoft Active Directory with license-m	Write	identity-provider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	anager-user-subscriptions for a product				
DisassociateUser	Grants permission to disassociate a subscribed user from an instance launched with license manager user subscriptions products	Write	identity-provider* instance-user*		
ListIdentityProviders	Grants permission to list all the identity providers on license manager user subscriptions	List			
ListInstances	Grants permission to list all the instances launched with license manager user subscription products	List			
ListLicenseServerEndpoints	Grants permission to list license server endpoints	List			
ListProductSubscriptions	Grants permission to lists all the product subscriptions for a product and identity provider	List	identity-provider*		
ListTagsForResource	Grants permission to list tags for a selected resource	Read	identity-provider* instance-user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			license-server-endpoint*		
			product-subscription*		
ListUserAssociations	Grants permission to list all the users associated to an instance launched for a product	List	identity-provider*		
RegisterIdentityProvider	Grants permission to registers Microsoft Active Directory with license-manager-user-subscriptions for a product	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StartProductSubscription	Grants permission to start product subscription for a user on a registered active directory for a product	Write	identity-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopProductSubscription	Grants permission to stop product subscription for a user on a registered active directory for a product	Write	identity-provider*		
			product-subscription*		
TagResource	Grants permission to tag a selected resource	Tagging	identity-provider*		
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a selected resource	Tagging	identity-provider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-user*		
			license-server-endpoint*		
			product-subscription*		
UpdateIdentityProviderSettings	Grants permission to update the identity provider configuration	Write	identity-provider*		

Resource types defined by AWS License Manager User Subscriptions

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
identity-provider	`arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:identity-provider/${IdentityProviderId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
product-subscription	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:product-subscription/${ProductSubscriptionId}	aws:ResourceTag/${TagKey}
instance-user	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:instance-user/${InstanceUserId}	aws:ResourceTag/${TagKey}
license-server-endpoint	arn:${Partition}:license-manager-user-subscriptions:${Region}:${Account}:license-server-endpoint/${LicenseServerEndpointId}	aws:ResourceTag/${TagKey}

Condition keys for AWS License Manager User Subscriptions

AWS License Manager User Subscriptions defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Lightsail

Amazon Lightsail (service prefix: `lightsail`) 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 Lightsail

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateStaticIp	Grants permission to create a static IP address that can be attached to an instance	Write			
AttachCertificateToDistribution	Grants permission to attach an SSL/TLS certificate to your Amazon Lightsail content delivery network (CDN) distribution	Write	Certificate* Distribution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachDisk	Grants permission to attach a disk to an instance	Write	Disk*		
AttachInstancesToLoadBalancer	Grants permission to attach one or more instances to a load balancer	Write	LoadBalancer*		
AttachLoadBalancerTlsCertificate	Grants permission to attach a TLS certificate to a load balancer	Write	LoadBalancer*		
AttachStaticIp	Grants permission to attach a static IP address to an instance	Write	Instance*		
			StaticIp*		
CloseInstancePublicPorts	Grants permission to close a public port of an instance	Write	Instance*		
CopySnapshot	Grants permission to copy a snapshot from one AWS Region to another in Amazon Lightsail	Write			
CreateBucket	Grants permission to create an Amazon Lightsail bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucketAccessKey	Grants permission to create a new access key for the specified bucket	Write	Bucket*		
CreateCertificate	Grants permission to create an SSL/TLS certificate	Write		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains
CreateCloudFormationStack	Grants permission to create a new Amazon EC2 instance from an exported Amazon Lightsail snapshot	Write			
CreateContactMethod	Grants permission to create an email or SMS text message contact method	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContainerService	Grants permission to create an Amazon Lightsail container service	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContainerServiceDeployment	Grants permission to create a deployment for your Amazon Lightsail container service	Write	ContainerService*		
CreateContainerServiceRegistryLogin	Grants permission to create a temporary set of log in credentials that you can use to log in to the Docker process on your local machine	Write			
CreateDisk	Grants permission to create a disk	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskFromSnapshot	Grants permission to create a disk from snapshot	Write	DiskSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDiskSnapshot	Grants permission to create a disk snapshot	Write	Disk		
			Instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDistribution	Grants permission to create an Amazon Lightsail content delivery network (CDN) distribution	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDomain	Grants permission to create a domain resource for the specified domain name	Write		aws:RequestTag/${TagKey} aws:TagKeys	route53:DeleteHostedZone route53:GetHostedZone route53:ListHostedZonesByName route53domains:GetDomainDetail route53domains:GetOperationDetail route53domains:ListDomains route53domains:ListOperations route53domains:Upd

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ateDomainNameservers
CreateDomainEntry	Grants permission to create one or more DNS record entries for a domain resource: Address (A), canonical name (CNAME), mail exchanger (MX), name server (NS), start of authority (SOA), service locator (SRV), or text (TXT)	Write	Domain*		
CreateGUISessionAccessDetails	Grants permission to create URLs that are used to access an instance's graphical user interface (GUI) session	Write	Instance*		
CreateInstanceSnapshot	Grants permission to create an instance snapshot	Write	Instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstances	Grants permission to create one or more instances	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInstancesFromSnapshot	Grants permission to create one or more instances based on an instance snapshot	Write	InstanceSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeyPair	Grants permission to create a key pair used to authenticate and connect to an instance	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoadBalancer	Grants permission to create a load balancer	Write		aws:RequestTag/${TagKey} aws:TagKeys	lightsail:CreateDomainEntry lightsail:GetDomains

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoadBalancerTlsCertificate	Grants permission to create a load balancer TLS certificate	Write	LoadBalancer*		lightsail:CreateDomainEntry lightsail:GetDomains
CreateRelationalDatabase	Grants permission to create a new relational database	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRelationalDatabaseFromSnapshot	Grants permission to create a new relational database from a snapshot	Write	RelationalDatabaseSnapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRelationalDatabaseSnapshot	Grants permission to create a relational database snapshot	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarm	Grants permission to delete an alarm	Write	Alarm*		
DeleteAutoSnapshot	Grants permission to delete an automatic snapshot of an instance or disk	Write			
DeleteBucket	Grants permission to delete an Amazon Lightsail bucket	Write	Bucket*		
DeleteBucketAccessKey	Grants permission to delete an access key for the specified Amazon Lightsail bucket	Write	Bucket*		
DeleteCertificate	Grants permission to delete an SSL/TLS certificate	Write	Certificate*		
DeleteContactMethod	Grants permission to delete a contact method	Write			
DeleteContainerImage	Grants permission to delete a container image that is registered to your Amazon Lightsail container service	Write	ContainerService*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContainerService	Grants permission to delete your Amazon Lightsail container service	Write	ContainerService*		
DeleteDisk	Grants permission to delete a disk	Write	Disk*		
DeleteDiskSnapshot	Grants permission to delete a disk snapshot	Write	DiskSnapshot*		
DeleteDistribution	Grants permission to delete your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution*		
DeleteDomain	Grants permission to delete a domain resource and all of its DNS records	Write	Domain*		
DeleteDomainEntry	Grants permission to delete a DNS record entry for a domain resource	Write	Domain*		
DeleteInstance	Grants permission to delete an instance	Write	Instance*		
DeleteInstanceSnapshot	Grants permission to delete an instance snapshot	Write	InstanceSnapshot*		
DeleteKeyPair	Grants permission to delete a key pair used to authenticate and connect to an instance	Write	KeyPair*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteKnownHostKeys	Grants permission to delete the known host key or certificate used by the Amazon Lightsail browser-based SSH or RDP clients to authenticate an instance	Write	Instance*		
DeleteLoadBalancer	Grants permission to delete a load balancer	Write	LoadBalancer*		
DeleteLoadBalancerTlsCertificate	Grants permission to delete a load balancer TLS certificate	Write	LoadBalancer*		
DeleteRelationalDatabase	Grants permission to delete a relational database	Write	RelationalDatabase*		
DeleteRelationalDatabaseSnapshot	Grants permission to delete a relational database snapshot	Write	RelationalDatabaseSnapshot*		
DetachCertificateFromDistribution	Grants permission to detach an SSL/TLS certificate from your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution*		
DetachDisk	Grants permission to detach a disk from an instance	Write	Disk*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachInstancesFromLoadBalancer	Grants permission to detach one or more instances from a load balancer	Write	LoadBalancer*		
DetachStaticIp	Grants permission to detach a static IP from an instance to which it is attached	Write	StaticIp*		
DisableAddOn	Grants permission to disable an add-on for an Amazon Lightsail resource	Write			
DownloadDefaultKeyPair	Grants permission to download the default key pair used to authenticate and connect to instances in a specific AWS Region	Write			
EnableAddOn	Grants permission to enable or modify an add-on for an Amazon Lightsail resource	Write			
ExportSnapshot	Grants permission to export an Amazon Lightsail snapshot to Amazon EC2	Write	DiskSnapshot		iam:CreateServiceLinkedRole iam:PutRolePolicy
			InstanceSnapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetActiveNames	Grants permission to get the names of all active (not deleted) resources	Read			
GetAlarms	Grants permission to view information about the configured alarms	Read			
GetAutoSnapshots	Grants permission to view the available automatic snapshots for an instance or disk	Read			
GetBlueprints	Grants permission to get a list of instance images, or blueprints. You can use a blueprint to create a new instance already running a specific operating system, as well as a pre-installed application or development stack. The software that runs on your instance depends on the blueprint you define when creating the instance	Read			
GetBucketAccessKeys	Grants permission to get the existing access key IDs for the specified Amazon Lightsail bucket	Read			
GetBucketBundles	Grants permission to get the bundles that can be applied to an Amazon Lightsail bucket	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketMetricData	Grants permission to get the data points of a specific metric for an Amazon Lightsail bucket	Read			
GetBuckets	Grants permission to get information about one or more Amazon Lightsail buckets	Read			
GetBundles	Grants permission to get a list of instance bundles. You can use a bundle to create a new instance with a set of performance specifications, such as CPU count, disk size, RAM size, and network transfer allowance. The cost of your instance depends on the bundle you define when creating the instance	Read			
GetCertificates	Grants permission to view information about one or more Amazon Lightsail SSL/TLS certificates	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCloudFormationStackRecords	Grants permission to get information about all CloudFormation stacks used to create Amazon EC2 resources from exported Amazon Lightsail snapshots	Read			
GetContactMethods	Grants permission to view information about the configured contact methods	Read			
GetContainerAPIMetadata	Grants permission to view information about Amazon Lightsail containers, such as the current version of the Lightsail Control (lightsailctl) plugin	Read			
GetContainerImages	Grants permission to view the container images that are registered to your Amazon Lightsail container service	Read			
GetContainerLog	Grants permission to view the log events of a container of your Amazon Lightsail container service	Read			
GetContainerServiceDeployments	Grants permission to view the deployments for your Amazon Lightsail container service	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContainerServiceMetricData	Grants permission to view the data points of a specific metric of your Amazon Lightsail container service	Read			
GetContainerServicePowers	Grants permission to view the list of powers that can be specified for your Amazon Lightsail container services	Read			
GetContainerServices	Grants permission to view information about one or more of your Amazon Lightsail container services	Read			
GetCostEstimate	Grants permission to get the information about the cost estimate for a specified resource	Read	Disk Instance		
GetDisk	Grants permission to get information about a disk	Read			
GetDiskSnapshot	Grants permission to get information about a disk snapshot	Read			
GetDiskSnapshots	Grants permission to get information about all disk snapshots	Read			
GetDisks	Grants permission to get information about all disks	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDistributionBundles	Grants permission to view the list of bundles that can be applied to you Amazon Lightsail content delivery network (CDN) distributions	Read			
GetDistributionLatestCacheReset	Grants permission to view the timestamp and status of the last cache reset of a specific Amazon Lightsail content delivery network (CDN) distribution	Read			
GetDistributionMetricData	Grants permission to view the data points of a specific metric for an Amazon Lightsail content delivery network (CDN) distribution	Read			
GetDistributions	Grants permission to view information about one or more of your Amazon Lightsail content delivery network (CDN) distributions	Read			
GetDomain	Grants permission to get DNS records for a domain resource	Read			
GetDomains	Grants permission to get DNS records for all domain resources	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExportSnapshotRecords	Grants permission to get information about all records of exported Amazon Lightsail snapshots to Amazon EC2	Read			
GetInstance	Grants permission to get information about an instance	Read			
GetInstanceAccessDetails	Grants permission to get temporary keys you can use to authenticate and connect to an instance	Write	Instance*		
GetInstanceMetricData	Grants permission to get the data points for the specified metric of an instance	Read			
GetInstancePortStates	Grants permission to get the port states of an instance	Read			
GetInstanceSnapshot	Grants permission to get information about an instance snapshot	Read			
GetInstanceSnapshots	Grants permission to get information about all instance snapshots	Read			
GetInstanceState	Grants permission to get the state of an instance	Read			
GetInstances	Grants permission to get information about all instances	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetKeyPair	Grants permission to get information about a key pair	Read			
GetKeyPairs	Grants permission to get information about all key pairs	Read			
GetLoadBalancer	Grants permission to get information about a load balancer	Read			
GetLoadBalancerMetricData	Grants permission to get the data points for the specified metric of a load balancer	Read			
GetLoadBalancerTlsCertificates	Grants permission to get information about a load balancer's TLS certificates	Read			
GetLoadBalancerTlsPolicies	Grants permission to get a list of TLS security policies that you can apply to Lightsail load balancers	Read			
GetLoadBalancers	Grants permission to get information about load balancers	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOperation	Grants permission to get information about an operation. Operations include events such as when you create an instance, allocate a static IP, attach a static IP, and so on	Read			
GetOperations	Grants permission to get information about all operations. Operations include events such as when you create an instance, allocate a static IP, attach a static IP, and so on	Read			
GetOperationsForResource	Grants permission to get operations for a resource	Read			
GetRegions	Grants permission to get a list of all valid AWS Regions for Amazon Lightsail	Read			
GetRelationalDatabase	Grants permission to get information about a relational database	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRelationalDatabaseBlueprints	Grants permission to get a list of relational database images, or blueprints. You can use a blueprint to create a new database running a specific database engine. The database engine that runs on your database depends on the blueprint you define when creating the relational database	Read			
GetRelationalDatabaseBundles	Grants permission to get a list of relational database bundles. You can use a bundle to create a new database with a set of performance specifications, such as CPU count, disk size, RAM size, network transfer allowance, and standard of high availability. The cost of your database depends on the bundle you define when creating the relational database	Read			
GetRelationalDatabaseEvents	Grants permission to get events for a relational database	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRelationalDatabaseLogEvents	Grants permission to get events for the specified log stream of a relational database	Read			
GetRelationalDatabaseLogStreams	Grants permission to get the log streams available for a relational database	Read			
GetRelationalDatabaseMasterUserPassword	Grants permission to get the master user password of a relational database	Write	RelationalDatabase*		
GetRelationalDatabaseMetricData	Grants permission to get the data points for the specified metric of a relational database	Read			
GetRelationalDatabaseParameters	Grants permission to get the parameters of a relational database	Read			
GetRelationalDatabaseSnapshot	Grants permission to get information about a relational database snapshot	Read			
GetRelationalDatabaseSnapshots	Grants permission to get information about all relational database snapshots	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRelationalDatabases	Grants permission to get information about all relational databases	Read			
GetSetupHistory	Grants permission to get detailed information for setup requests that were run on the specified resource	Read	Instance		
GetStaticIp	Grants permission to get information about a static IP	Read			
GetStaticIps	Grants permission to get information about all static IPs	Read			
ImportKeyPair	Grants permission to import a public key from a key pair	Write			
IsVpcPeered	Grants permission to get a boolean value indicating whether the Amazon Lightsail virtual private cloud (VPC) is peered	Read			
OpenInstancePublicPorts	Grants permission to add, or open a public port of an instance	Write	Instance*		
PeerVpc	Grants permission to try to peer the Amazon Lightsail virtual private cloud (VPC) with the default VPC	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAlarm	Grants permission to creates or update an alarm, and associate it with the specified metric	Write	Alarm*		
PutInstancePublicPorts	Grants permission to set the specified open ports for an instance, and closes all ports for every protocol not included in the request	Write	Instance*		
RebootInstance	Grants permission to reboot an instance that is in a running state	Write	Instance*		
RebootRelationalDatabase	Grants permission to reboot a relational database that is in a running state	Write	RelationalDatabase*		
RegisterContainerImage	Grants permission to register a container image to your Amazon Lightsail container service	Write	ContainerService*		
ReleaseStaticIp	Grants permission to delete a static IP	Write	StaticIp*		
ResetDistributionCache	Grants permission to delete currently cached content from your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendContactMethodVerification	Grants permission to send a verification request to an email contact method to ensure it's owned by the requester	Write			
SetIpAddressType	Grants permission to set the IP address type for a Amazon Lightsail resource	Write	Distribution		
			Instance		
			LoadBalancer		
SetResourceAccessForBucket	Grants permission to set the Amazon Lightsail resources that can access the specified Amazon Lightsail bucket	Write	Bucket*		
			Instance*		
SetupInstanceHttps	Grants permission to create an SSL/TLS certificate and install it on a specified instance	Write	Instance*		lightsail:GetInstanceAccessDetails
StartGUISession	Grants permission to initiate a graphical user interface (GUI) session used to access an instance's operating system or application	Write	Instance*		
StartInstance	Grants permission to start an instance that is in a stopped state	Write	Instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartRelationalDatabase	Grants permission to start a relational database that is in a stopped state	Write	RelationalDatabase*		
StopGUISession	Grants permission to terminate a graphical user interface (GUI) session used to access an instance's operating system or application	Write	Instance*		
StopInstance	Grants permission to stop an instance that is in a running state	Write	Instance*		
StopRelationalDatabase	Grants permission to stop a relational database that is in a running state	Write	RelationalDatabase*		
TagResource	Grants permission to tag a resource	Tagging	Bucket		
			Certificate		
			ContactMethod		
			ContainerService		
			Disk		
			DiskSnapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Distribution		
			Domain		
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestAlarm	Grants permission to test an alarm by displaying a banner on the Amazon Lightsail console or if a notification trigger is configured for the specified alarm, by sending a notification to the notification protocol	Write	Alarm*		
UnpeerVpc	Grants permission to try to unpeer the Amazon Lightsail virtual private cloud (VPC) from the default VPC	Write			
UntagResource	Grants permission to untag a resource	Tagging	Bucket		
			Certificate		
			ContactMethod		
			ContainerService		
			Disk		
			DiskSnapshot		
			Distribution		
			Domain		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Instance		
			InstanceSnapshot		
			KeyPair		
			LoadBalancer		
			RelationalDatabase		
			RelationalDatabaseSnapshot		
			StaticIp		
				aws:TagKeys	
UpdateBucket	Grants permission to update an existing Amazon Lightsail bucket	Write	Bucket*		
UpdateBucketBundle	Grants permission to update the bundle, or storage plan, of an existing Amazon Lightsail bucket	Write	Bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContainerService	Grants permission to update the configuration of your Amazon Lightsail container service, such as its power, scale, and public domain names	Write	ContainerService*		
UpdateDistribution	Grants permission to update an existing Amazon Lightsail content delivery network (CDN) distribution or its configuration	Write	Distribution*		
UpdateDistributionBundle	Grants permission to update the bundle of your Amazon Lightsail content delivery network (CDN) distribution	Write	Distribution*		
UpdateDomainEntry	Grants permission to update a domain recordset after it is created	Write	Domain*		
UpdateInstanceMetadataOptions	Grants permission to update metadata options for an instance	Write	Instance*		
UpdateLoadBalancerAttribute	Grants permission to update a load balancer attribute, such as the health check path and session stickiness	Write	LoadBalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRelationalDatabase	Grants permission to update a relational database	Write	RelationalDatabase*		
UpdateRelationalDatabaseParameters	Grants permission to update the parameters of a relational database	Write	RelationalDatabase*		

Resource types defined by Amazon Lightsail

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:${Partition}:lightsail:${Region}:${Account}:Domain/${Id}`	aws:ResourceTag/${TagKey}
Instance	`arn:${Partition}:lightsail:${Region}:${Account}:Instance/${Id}`	aws:ResourceTag/${TagKey}
InstanceSnapshot	`arn:${Partition}:lightsail:${Region}:${Account}:InstanceSnapshot/${Id}`	aws:ResourceTag/${TagKey}
KeyPair	`arn:${Partition}:lightsail:${Region}:${Account}:KeyPair/${Id}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
StaticIp	arn:${Partition}:lightsail:${Region}:${Account}:StaticIp/${Id}	aws:ResourceTag/${TagKey}
Disk	arn:${Partition}:lightsail:${Region}:${Account}:Disk/${Id}	aws:ResourceTag/${TagKey}
DiskSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:DiskSnapshot/${Id}	aws:ResourceTag/${TagKey}
LoadBalancer	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancer/${Id}	aws:ResourceTag/${TagKey}
LoadBalancerTlsCertificate	arn:${Partition}:lightsail:${Region}:${Account}:LoadBalancerTlsCertificate/${Id}	
ExportSnapshotRecord	arn:${Partition}:lightsail:${Region}:${Account}:ExportSnapshotRecord/${Id}	
CloudFormationStackRecord	arn:${Partition}:lightsail:${Region}:${Account}:CloudFormationStackRecord/${Id}	
RelationalDatabase	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabase/${Id}	aws:ResourceTag/${TagKey}
RelationalDatabaseSnapshot	arn:${Partition}:lightsail:${Region}:${Account}:RelationalDatabaseSnapshot/${Id}	aws:ResourceTag/${TagKey}
Alarm	arn:${Partition}:lightsail:${Region}:${Account}:Alarm/${Id}	
Certificate	arn:${Partition}:lightsail:${Region}:${Account}:Certificate/${Id}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ContactMethod	arn:${Partition}:lightsail:${Region}:${Account}:ContactMethod/${Id}	aws:ResourceTag/${TagKey}
ContainerService	arn:${Partition}:lightsail:${Region}:${Account}:ContainerService/${Id}	aws:ResourceTag/${TagKey}
Distribution	arn:${Partition}:lightsail:${Region}:${Account}:Distribution/${Id}	aws:ResourceTag/${TagKey}
Bucket	arn:${Partition}:lightsail:${Region}:${Account}:Bucket/${Id}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Lightsail

Amazon Lightsail defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Location

Amazon Location (service prefix: geo) 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 Location

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTrackerConsumer	Grants permission to create an association between a geofence-collection and a tracker resource	Write	tracker*		
BatchDeleteDevicePositionHistory	Grants permission to delete a batch of device position histories from a tracker resource	Write	tracker*		
				geo:DeviceIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteGeofence	Grants permission to delete a batch of geofences from a geofence collection	Write	geofence-collection*		
				geo:GeofenceIds	
BatchEvaluateGeofences	Grants permission to evaluate device positions against the position of geofences in a given geofence collection	Write	geofence-collection*		
BatchGetDevicePosition	Grants permission to send a batch request to retrieve device positions	Read	tracker*		
				geo:DeviceIds	
BatchPutGeofence	Grants permission to send a batch request for adding geofences into a given geofence collection	Write	geofence-collection*		
				geo:GeofenceIds	
BatchUpdateDevicePosition	Grants permission to upload a position update for one or more devices to a tracker resource	Write	tracker*		
				geo:DeviceIds	
CalculateRoute	Grants permission to calculate routes using a given route calculator resource	Read	route-calculator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CalculateRouteMatrix	Grants permission to calculate a route matrix using a given route calculator resource	Read	route-calculator*		
CreateGeofenceCollection	Grants permission to create a geofence-collection	Write	geofence-collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKey	Grants permission to create an API key resource	Write	api-key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMap	Grants permission to create a map resource	Write	map*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlaceIndex	Grants permission to create a place index resource	Write	place-index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRouteCalculator	Grants permission to create a route calculator resource	Write	route-calculator*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTracker	Grants permission to create a tracker resource	Write	tracker*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGeofenceCollection	Grants permission to delete a geofence-collection	Write	geofence-collection*		
DeleteKey	Grants permission to delete an API key resource	Write	api-key*		
DeleteMap	Grants permission to delete a map resource	Write	map*		
DeletePlaceIndex	Grants permission to delete a place index resource	Write	place-index*		
DeleteRouteCalculator	Grants permission to delete a route calculator resource	Write	route-calculator*		
DeleteTracker	Grants permission to delete a tracker resource	Write	tracker*		
DescribeGeofenceCollection	Grants permission to retrieve geofence collection details	Read	geofence-collection*		
DescribeKey	Grants permission to retrieve API key resource details and secret	Read	api-key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMap	Grants permission to retrieve map resource details	Read	map*		
DescribePlaceIndex	Grants permission to retrieve place-index resource details	Read	place-index*		
DescribeRouteCalculator	Grants permission to retrieve route calculator resource details	Read	route-calculator*		
DescribeTracker	Grants permission to retrieve a tracker resource details	Read	tracker*		
DisassociateTrackerConsumer	Grants permission to remove the association between a tracker resource and a geofence-collection	Write	tracker*		
ForecastGeofenceEvents	Grants permission to forecast events for geofences stored in a given geofence collection	Read	geofence-collection*		
GetDevicePosition	Grants permission to retrieve the latest device position	Read	tracker*		
				geo:DeviceIds	
GetDevicePositionHistory	Grants permission to retrieve the device position history	Read	tracker*		
				geo:DeviceIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGeofence	Grants permission to retrieve the geofence details from a geofence-collection	Read	geofence-collection*		
				geo:GeofenceIds	
GetMapGlyphs	Grants permission to retrieve the glyph file for a map resource	Read	map*		
GetMapSprites	Grants permission to retrieve the sprite file for a map resource	Read	map*		
GetMapStyleDescriptor	Grants permission to retrieve the map style descriptor from a map resource	Read	map*		
GetMapTile	Grants permission to retrieve the map tile from the map resource	Read	map*		
GetPlace	Grants permission to find a place by its unique ID	Read	place-index*		
ListDevicePositions	Grants permission to retrieve a list of devices and their latest positions from the given tracker resource	Read	tracker*		
ListGeofenceCollections	Grants permission to lists geofence-collections	List	geofence-collection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGeofences	Grants permission to list geofences stored in a given geofence collection	Read	geofence-collection*		
ListKeys	Grants permission to list API key resources	List	api-key*		
ListMaps	Grants permission to list map resources	List	map*		
ListPlaceIndexes	Grants permission to return a list of place index resources	List	place-index*		
ListRouteCalculators	Grants permission to return a list of route calculator resources	List	route-calculator*		
ListTagsForResource	Grants permission to list the tags (metadata) which you have assigned to the resource	Read	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrackerConsumers	Grants permission to retrieve a list of geofence collections currently associated to the given tracker resource	Read	tracker*		
ListTrackers	Grants permission to return a list of tracker resources	List	tracker*		
PutGeofence	Grants permission to add a new geofence or update an existing geofence to a given geofence-collection	Write	geofence-collection*		
				geo:GeofenceIds	
SearchPlaceIndexForPosition	Grants permission to reverse geocodes a given coordinate	Read	place-index*		
SearchPlaceIndexForSuggestions	Grants permission to generate suggestions for addresses and points of interest based on partial or misspelled free-form text	Read	place-index*		
SearchPlaceIndexForText	Grants permission to geocode free-form text, such as an address, name, city or region	Read	place-index*		
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	api-key		
			geofence-collection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			map		
			place-index		
			route-calculator		
			tracker		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the given tags (metadata) from the resource	Tagging	api-key		
			geofence-collection		
			map		
			place-index		
			route-calculator		
			tracker		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateGeofenceCollection	Grants permission to update a geofence collection	Write	geofence-collection*		
UpdateKey	Grants permission to update an API key resource	Write	api-key*		
UpdateMap	Grants permission to update a map resource	Write	map*		
UpdatePlaceIndex	Grants permission to update a place index resource	Write	place-index*		
UpdateRouteCalculator	Grants permission to update a route calculator resource	Write	route-calculator*		
UpdateTracker	Grants permission to update a tracker resource	Write	tracker*		
VerifyDevicePosition	Grants permission to verify a device position	Read	tracker*		
				geo:DeviceIds	

Resource types defined by Amazon Location

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
api-key	arn:${Partition}:geo:${Region}:${Account}:api-key/${KeyName}	aws:ResourceTag/${TagKey}
geofence-collection	arn:${Partition}:geo:${Region}:${Account}:geofence-collection/${GeofenceCollectionName}	aws:ResourceTag/${TagKey} geo:GeofenceIds
map	arn:${Partition}:geo:${Region}:${Account}:map/${MapName}	aws:ResourceTag/${TagKey}
place-index	arn:${Partition}:geo:${Region}:${Account}:place-index/${IndexName}	aws:ResourceTag/${TagKey}
route-calculator	arn:${Partition}:geo:${Region}:${Account}:route-calculator/${CalculatorName}	aws:ResourceTag/${TagKey}
tracker	arn:${Partition}:geo:${Region}:${Account}:tracker/${TrackerName}	aws:ResourceTag/${TagKey} geo:DeviceIds

Condition keys for Amazon Location

Amazon Location defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag's key and value in a request	String
aws:ResourceTag/${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
geo:DeviceIds	Filters access by the presence of device ids in the request	ArrayOfString
geo:GeofenceIds	Filters access by the presence of geofence ids in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Location Service Maps

Amazon Location Service Maps (service prefix: `geo-maps`) 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 Location Service Maps
- Resource types defined by Amazon Location Service Maps
- Condition keys for Amazon Location Service Maps

Actions defined by Amazon Location Service Maps

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStaticMap	Grants permission to retrieve the static map	Read	provider*		
GetTile	Grants permission to retrieve the map tile	Read	provider*		

Resource types defined by Amazon Location Service Maps

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
provider	`arn:${Partition}:geo-maps:${Region}::provider/default`	

Condition keys for Amazon Location Service Maps

Geo Maps has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Location Service Places

Amazon Location Service Places (service prefix: `geo-places`) 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 Location Service Places

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Autocomplete	Grants permission to autocomplete text input with potential places and addresses as the user types	Read	provider*		
Geocode	Grants permission to geocode a textual address or place into geographic coordinates	Read	provider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPlace	Grants permission to query a place by it's unqiue place ID	Read	provider*		
ReverseGeocode	Grants permission to convert geographic coordinates into a human-readable address or place	Read	provider*		
SearchNearby	Grants permission to retrieve places near a position which match to a set of user defined restrictions such as category or food type offered by the place	Read	provider*		
SearchText	Grants permission to query for places using a single free-form text input	Read	provider*		
Suggest	Grants permission to suggest potential places based on the user's input	Read	provider*		

Resource types defined by Amazon Location Service Places

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
provider	arn:${Partition}:geo-places:${Region}::provider/default	

Condition keys for Amazon Location Service Places

Geo Places has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Location Service Routes

Amazon Location Service Routes (service prefix: geo-routes) 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 Location Service Routes
- Resource types defined by Amazon Location Service Routes
- Condition keys for Amazon Location Service Routes

Actions defined by Amazon Location Service Routes

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CalculateIsolines	Grants permission to determine destinations or service areas reachable within a specified time	Read	provider*		
CalculateRouteMatrix	Grants permission to calculate routing matrice which providing travel time and distances between sets of origins and destinations	Read	provider*		
CalculateRoutes	Grants permission to calculates routes between two or more locations	Read	provider*		
OptimizeWaypoints	Grants permission to calculate the most efficient sequence for visiting multiple waypoints or locations along a route	Read	provider*		
SnapToRoads	Grants permission to enhances the accuracy of geographic positioning by aligning GPS coordinates to the nearest road segments on a digital map	Read	provider*		

Resource types defined by Amazon Location Service Routes

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
provider	`arn:${Partition}:geo-routes:${Region}::provider/default`	

Condition keys for Amazon Location Service Routes

Geo Routes has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Lookout for Equipment

Amazon Lookout for Equipment (service prefix: `lookoutequipment`) 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 Lookout for Equipment
- Resource types defined by Amazon Lookout for Equipment
- Condition keys for Amazon Lookout for Equipment

Actions defined by Amazon Lookout for Equipment

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataset	Grants permission to create a dataset	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceScheduler	Grants permission to create an inference scheduler for a trained model	Write	inference-scheduler*		
			model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabel	Grants permission to create a label	Write	label-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLabelGroup	Grants permission to create a label group	Write	label-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Grants permission to create a model that is trained on a dataset	Write	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRetrainingScheduler	Grants permission to create a retraining scheduler for a trained model	Write	model*		
DeleteDataset	Grants permission to delete a dataset	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInferenceScheduler	Grants permission to delete an inference scheduler	Write	inference-scheduler*		
DeleteLabel	Grants permission to delete a label	Write	label-group*		
DeleteLabelGroup	Grants permission to delete a label group	Write	label-group*		
DeleteModel	Grants permission to delete a model	Write	model*		
DeleteResourcePolicy	Grants permission to delete a resource policy	Write	dataset		
			model		
			model-version		
DeleteRetrainingScheduler	Grants permission to delete a retraining scheduler of a trained model	Write	model*		
DescribeDataIngestionJob	Grants permission to describe a data ingestion job	Read			
DescribeDataset	Grants permission to describe a dataset	Read	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInferenceScheduler	Grants permission to describe an inference scheduler	Read	inference-scheduler*		
DescribeLabelGroup	Grants permission to describe a label group	Read	label-group*		
DescribeModel	Grants permission to describe a model	Read	model*		
DescribeModelVersion	Grants permission to describe a model version	Read	model-version*		
DescribeResourcePolicy	Grants permission to describe a resource policy	Read	dataset		
			model		
			model-version		
DescribeRetrainingScheduler	Grants permission to describe a retraining scheduler of a trained model	Read	model*		
Describelabel	Grants permission to describe a label	Read	label-group*		
ImportDataset	Grants permission to import a dataset	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ImportModelVersion	Grants permission to import a model version	Write	dataset*		
			model*		
			label-group		
				aws:RequestTag/${TagKey} aws:TagKeys lookoutequipment:IsImportingData	
ListDataIngestionJobs	Grants permission to list the data ingestion jobs in your account or for a particular dataset	List	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatasets	Grants permission to list the datasets in your account	List			
ListInferenceEvents	Grants permission to list the inference events for an inference scheduler	Read	inference-scheduler*		
ListInferenceExecutions	Grants permission to list the inference executions for an inference scheduler	Read	inference-scheduler*		
ListInferenceSchedulers	Grants permission to list the inference schedulers in your account	List			
ListLabelGroups	Grants permission to list the label groups in your account	List	label-group*		
ListLabels	Grants permission to list the labels in your account	List	label-group*		
ListModelVersions	Grants permission to list the model versions in your account	List	model*		
ListModels	Grants permission to list the models in your account	List			
ListRetrainingSchedulers	Grants permission to list the retraining schedulers in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSensorStatistics	Grants permission to list the sensor statistics for a particular dataset or an ingestion job	List	dataset*		
ListTagsForResource	Grants permission to list the tags for a resource	Read	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
PutResourcePolicy	Grants permission to put a resource policy	Write	dataset		
			model		
			model-version		
StartDataIngestionJob	Grants permission to start a data ingestion job for a dataset	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInferenceScheduler	Grants permission to start an inference scheduler	Write	inference-scheduler*		
StartRetrainingScheduler	Grants permission to start a retraining scheduler of a trained model	Write	model*		
StopInferenceScheduler	Grants permission to stop an inference scheduler	Write	inference-scheduler*		
StopRetrainingScheduler	Grants permission to stop a retraining scheduler of a trained model	Write	model*		
TagResource	Grants permission to tag a resource	Tagging	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	dataset		
			inference-scheduler		
			label-group		
			model		
			model-version		
				aws:TagKeys	
UpdateActiveModelVersion	Grants permission to set the active model version for a given machine learning model	Write	model*		
			model-version*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInferenceScheduler	Grants permission to update an inference scheduler	Write	inference-scheduler*		
UpdateLabelGroup	Grants permission to update a label group	Write	label-group*		
UpdateModel	Grants permission to update a trained model	Write	model*		
UpdateRetrainingScheduler	Grants permission to update a retraining scheduler of a trained model	Write	model*		

Resource types defined by Amazon Lookout for Equipment

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
dataset	`arn:${Partition}:lookoutequipment:${Region}:${Account}:dataset/${DatasetName}/${DatasetId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
model	arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}	aws:ResourceTag/${TagKey}
model-version	arn:${Partition}:lookoutequipment:${Region}:${Account}:model/${ModelName}/${ModelId}/model-version/${ModelVersionNumber}	aws:ResourceTag/${TagKey}
inference-scheduler	arn:${Partition}:lookoutequipment:${Region}:${Account}:inference-scheduler/${InferenceSchedulerName}/${InferenceSchedulerId}	aws:ResourceTag/${TagKey}
label-group	arn:${Partition}:lookoutequipment:${Region}:${Account}:label-group/${LabelGroupName}/${LabelGroupId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Lookout for Equipment

Amazon Lookout for Equipment defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
lookoutequipment:IsImportingData	Filters access by the import strategy of underlying data	Bool

Actions, resources, and condition keys for Amazon Lookout for Metrics

Amazon Lookout for Metrics (service prefix: `lookoutmetrics`) 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 Lookout for Metrics
- Resource types defined by Amazon Lookout for Metrics
- Condition keys for Amazon Lookout for Metrics

Actions defined by Amazon Lookout for Metrics

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateAnomalyDetector	Grants permission to activate an anomaly detector	Write	AnomalyDetector*		
BackTestAnomalyDetector	Grants permission to run a backtest with an anomaly detector	Write	AnomalyDetector*		
CreateAlert	Grants permission to create an alert for an anomaly detector	Write	Alert*		
			AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalyDetector	Grants permission to create an anomaly detector	Write	AnomalyDetector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetricSet	Grants permission to create a dataset	Write	AnomalyDetector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			MetricSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateAnomalyDetector	Grants permission to deactivate an anomaly detector	Write	AnomalyDetector*		
DeleteAlert	Grants permission to delete an alert	Write	Alert*		
DeleteAnomalyDetector	Grants permission to delete an anomaly detector	Write	AnomalyDetector*		
DescribeAlert	Grants permission to get details about an alert	Read	Alert*		
DescribeAnomalyDetectionExecutions	Grants permission to get information about an anomaly detection job	Read	AnomalyDetector*		
DescribeAnomalyDetector	Grants permission to get details about an anomaly detector	Read	AnomalyDetector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMetricSet	Grants permission to get details about a dataset	Read	MetricSet*		
DetectMetricSetConfig	Grants permission to detect metric set config from data source	Write	AnomalyDetector*		
GetAnomalyGroup	Grants permission to get details about a group of affected metrics	Read	AnomalyDetector*		
GetDataQualityMetrics	Grants permission to get data quality metrics for an anomaly detector	Read	AnomalyDetector*		
GetFeedback	Grants permission to get feedback on affected metrics for an anomaly group	Read	AnomalyDetector*		
GetSampleData	Grants permission to get a selection of sample records from an Amazon S3 datasource	Read			
ListAlerts	Grants permission to get a list of alerts for a detector	List	AnomalyDetector		
ListAnomalyDetectors	Grants permission to get a list of anomaly detectors	List			
ListAnomalyGroupRelatedMetrics	Grants permission to get a list of related measures in an anomaly group	List	AnomalyDetector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAnomalyGroupSummaries	Grants permission to get a list of anomaly groups	List	AnomalyDetector*		
ListAnomalyGroupTimeSeries	Grants permission to get a list of affected metrics for a measure in an anomaly group	List	AnomalyDetector*		
ListMetricSets	Grants permission to get a list of datasets	List	AnomalyDetector		
ListTagsForResource	Grants permission to get a list of tags for a detector, dataset, or alert	Read	Alert		
			AnomalyDetector		
			MetricSet		
PutFeedback	Grants permission to add feedback for an affected metric in an anomaly group	Write	AnomalyDetector*		
TagResource	Grants permission to add tags to a detector, dataset, or alert	Tagging	Alert		
			AnomalyDetector		
			MetricSet		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from a detector, dataset, or alert	Tagging	Alert		
			AnomalyDetector		
			MetricSet		
				aws:TagKeys	
UpdateAlert	Grants permission to update an alert for an anomaly detector	Write	Alert*		
UpdateAnomalyDetector	Grants permission to update an anomaly detector	Write	AnomalyDetector*		
UpdateMetricSet	Grants permission to update a dataset	Write	MetricSet*		

Resource types defined by Amazon Lookout for Metrics

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
AnomalyDetector	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:AnomalyDetector:${AnomalyDetectorName}`	aws:ResourceTag/${TagKey}
MetricSet	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:MetricSet/${AnomalyDetectorName}/${MetricSetName}`	aws:ResourceTag/${TagKey}
Alert	`arn:${Partition}:lookoutmetrics:${Region}:${Account}:Alert:${AlertName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Lookout for Metrics

Amazon Lookout for Metrics defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Lookout for Vision

Amazon Lookout for Vision (service prefix: `lookoutvision`) 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 Lookout for Vision
- Resource types defined by Amazon Lookout for Vision
- Condition keys for Amazon Lookout for Vision

Actions defined by Amazon Lookout for Vision

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataset	Grants permission to create a dataset manifest	Write			
CreateModel	Grants permission to create a new anomaly detection model	Write	model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Grants permission to create a new project	Write	project*		
DeleteDataset	Grants permission to delete a dataset	Write			
DeleteModel	Grants permission to delete a model and all associated assets	Write	model*		
DeleteProject	Grants permission to permanently remove a project	Write	project*		
DescribeDataset	Grants permission to show detailed information about dataset manifest	Read			
DescribeModel	Grants permission to show detailed information about a model	Read	model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelPackagingJob	Grants permission to show detailed information about a model packaging job	Read			
DescribeProject	Grants permission to show detailed information about a project	Read	project*		
DescribeTrialDetection [permission only]	Grants permission to provides state information about a running anomaly detection job	Read			
DetectAnomalies	Grants permission to invoke detection of anomalies	Write	model*		
ListDatasetEntries	Grants permission to list the contents of dataset manifest	Read			
ListModelPackagingJobs	Grants permission to list all model packaging jobs associated with a project	List			
ListModels	Grants permission to list all models associated with a project	List			
ListProjects	Grants permission to list all projects	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	model		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrialDetections [permission only]	Grants permission to list all anomaly detection jobs	List			
StartModel	Grants permission to start anomaly detection model	Write	model*		
StartModelPackagingJob	Grants permission to start a model packaging job	Write	model*		
StartTrialDetection [permission only]	Grants permission to start bulk detection of anomalies for a set of images stored in an S3 bucket	Write			
StopModel	Grants permission to stop anomaly detection model	Write	model*		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	model		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	model		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDatasetEntries	Grants permission to update a training or test dataset manifest	Write			

Resource types defined by Amazon Lookout for Vision

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
model	`arn:${Partition}:lookoutvision:${Region}:${Account}:model/${ProjectName}/${ModelVersion}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:lookoutvision:${Region}:${Account}:project/${ProjectName}`	

Condition keys for Amazon Lookout for Vision

Amazon Lookout for Vision defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Machine Learning

Amazon Machine Learning (service prefix: `machinelearning`) 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 Machine Learning
- Resource types defined by Amazon Machine Learning
- Condition keys for Amazon Machine Learning

Actions defined by Amazon Machine Learning

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTags	Adds one or more tags to an object, up to a limit of 10. Each tag consists of a key and an optional value	Tagging	batchprediction		
			datasource		
			evaluation		
			mlmodel		
CreateBatchPrediction	Generates predictions for a group of observations	Write	batchprediction*		
			datasource*		
			mlmodel*		
CreateDataSourceFromRDS	Creates a DataSource object from an Amazon RDS	Write	datasource*		
CreateDataSourceFromRedshift	Creates a DataSource from a database hosted on an Amazon Redshift cluster	Write	datasource*		
CreateDataSourceFromS3	Creates a DataSource object from S3	Write	datasource*		
CreateEvaluation	Creates a new Evaluation of an MLModel	Write	datasource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			evaluation*		
			mlmodel*		
CreateMLModel	Creates a new MLModel	Write	datasource*		
			mlmodel*		
CreateRealtimeEndpoint	Creates a real-time endpoint for the MLModel	Write	mlmodel*		
DeleteBatchPrediction	Assigns the DELETED status to a BatchPrediction, rendering it unusable	Write	batchprediction*		
DeleteDataSource	Assigns the DELETED status to a DataSource, rendering it unusable	Write	datasource*		
DeleteEvaluation	Assigns the DELETED status to an Evaluation, rendering it unusable	Write	evaluation*		
DeleteMLModel	Assigns the DELETED status to an MLModel, rendering it unusable	Write	mlmodel*		
DeleteRealtimeEndpoint	Deletes a real time endpoint of an MLModel	Write	mlmodel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTags	Deletes the specified tags associated with an ML object. After this operation is complete, you can't recover deleted tags	Tagging	batchprediction		
			datasource		
			evaluation		
			mlmodel		
DescribeBatchPredictions	Returns a list of BatchPrediction operations that match the search criteria in the request	List			
DescribeDataSources	Returns a list of DataSource that match the search criteria in the request	List			
DescribeEvaluations	Returns a list of DescribeEvaluations that match the search criteria in the request	List			
DescribeMLModels	Returns a list of MLModel that match the search criteria in the request	List			
DescribeTags	Describes one or more of the tags for your Amazon ML object	List	batchprediction		
			datasource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			evaluation		
			mlmodel		
GetBatchPrediction	Returns a BatchPrediction that includes detailed metadata, status, and data file information	Read	batchprediction*		
GetDataSource	Returns a DataSource that includes metadata and data file information, as well as the current status of the DataSource	Read	datasource*		
GetEvaluation	Returns an Evaluation that includes metadata as well as the current status of the Evaluation	Read	datasource*		
GetMLModel	Returns an MLModel that includes detailed metadata, and data source information as well as the current status of the MLModel	Read	mlmodel*		
Predict	Generates a prediction for the observation using the specified ML Model	Write	mlmodel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBatchPrediction	Updates the BatchPredictionName of a BatchPrediction	Write	batchprediction*		
UpdateDataSource	Updates the DataSourceName of a DataSource	Write	datasource*		
UpdateEvaluation	Updates the EvaluationName of an Evaluation	Write	evaluation*		
UpdateMLModel	Updates the MLModelName and the ScoreThreshold of an MLModel	Write	mlmodel*		

Resource types defined by Amazon Machine Learning

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
batchprediction	`arn:${Partition}:machinelearning:${Region}:${Account}:batchprediction/${BatchPredictionId}`	
datasource	`arn:${Partition}:machinelearning:${Region}:${Account}:datasource/${DatasourceId}`	

Resource types	ARN	Condition keys
evaluation	arn:${Partition}:machinelearning:${Region}:${Account}:evaluation/${EvaluationId}	
mlmodel	arn:${Partition}:machinelearning:${Region}:${Account}:mlmodel/${MlModelId}	

Condition keys for Amazon Machine Learning

Machine Learning has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Macie

Amazon Macie (service prefix: macie2) 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 Macie
- Resource types defined by Amazon Macie
- Condition keys for Amazon Macie

Actions defined by Amazon Macie

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

The DisassociateFromMasterAccount and GetMasterAccount actions have been deprecated. We recommend that you specify the DisassociateFromAdministratorAccount and GetAdministratorAccount actions respectively instead.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptInvitation	Grants permission to accept an Amazon Macie membership invitation	Write			
BatchGetCustomDataIdentifiers	Grants permission to retrieve information about one or more custom data identifiers	Read	CustomDataIdentifier*		
BatchUpdateAutomatedDiscoveryAccounts	Grants permission to an Amazon Macie administrator to change the status of automated sensitive data discovery for one or more accounts in their organization	Write			
CreateAllowList	Grants permission to create and define the settings for an allow list	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateClassificationJob	Grants permission to create and define the settings for a sensitive data discovery job	Write	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDataIdentifier	Grants permission to create and define the settings for a custom data identifier	Write	CustomDataIdentifier*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsFilter	Grants permission to create and define the settings for a findings filter	Write	FindingsFilter*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvitations	Grants permission to send an Amazon Macie membership invitation	Write			
CreateMember	Grants permission to associate an account with an Amazon Macie administrator account	Write	Member*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSampleFindings	Grants permission to create sample findings	Write			
DeclineInvitations	Grants permission to decline Amazon Macie membership invitations	Write			
DeleteAllowList	Grants permission to delete an allow list	Write	AllowList*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomDataIdentifier	Grants permission to delete a custom data identifier	Write	CustomDataIdentifier*		
DeleteFindingsFilter	Grants permission to delete a findings filter	Write	FindingsFilter*		
DeleteInvitations	Grants permission to delete Amazon Macie membership invitations	Write			
DeleteMember	Grants permission to delete the association between an Amazon Macie administrator account and an account	Write	Member*		
DescribeBuckets	Grants permission to retrieve statistical data and other information about S3 buckets that Amazon Macie monitors and analyzes	Read			
DescribeClassificationJob	Grants permission to retrieve information about the status and settings for a sensitive data discovery job	Read	ClassificationJob*		
DescribeOrganizationConfiguration	Grants permission to retrieve information about the Amazon Macie configuration settings for an AWS organization	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableMacie	Grants permission to disable an Amazon Macie account, which also deletes Macie resources for the account	Write			
DisableOrganizationAdminAccount	Grants permission to disable an account as the delegated Amazon Macie administrator account for an AWS organization	Write			
DisassociateFromAdministratorAccount	Grants permission to an Amazon Macie member account to disassociate from its Macie administrator account	Write			
DisassociateFromMasterAccount	Grants permission to an Amazon Macie member account to disassociate from its Macie administrator account	Write			
DisassociateMember	Grants permission to an Amazon Macie administrator account to disassociate from a Macie member account	Write	Member*		
EnableMacie	Grants permission to enable and specify the configuration settings for a new Amazon Macie account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOrganizationAdminAccount	Grants permission to enable an account as the delegated Amazon Macie administrator account for an AWS organization	Write			
GetAdministratorAccount	Grants permission to retrieve information about the Amazon Macie administrator account for an account	Read			
GetAllowList	Grants permission to retrieve the settings and status of an allow list	Read	AllowList *		
GetAutomatedDiscoveryConfiguration	Grants permission to retrieve the configuration settings and status of automated sensitive data discovery for an Amazon Macie administrator account, organization, or standalone account	Read			
GetBucketStatistics	Grants permission to retrieve aggregated statistical data for all the S3 buckets that Amazon Macie monitors and analyzes	Read			
GetClassificationExportConfiguration	Grants permission to retrieve the settings for exporting sensitive data discovery results	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetClassificationScope	Grants permission to retrieve the classification scope settings for an account	Read			
GetCustomDataIdentifier	Grants permission to retrieve information about the settings for a custom data identifier	Read	CustomDataIdentifier*		
GetFindingStatistics	Grants permission to retrieve aggregated statistical data about findings	Read			
GetFindings	Grants permission to retrieve the details of one or more findings	Read			
GetFindingsFilter	Grants permission to retrieve information about the settings for a findings filter	Read	FindingsFilter*		
GetFindingsPublicationConfiguration	Grants permission to retrieve the configuration settings for publishing findings to AWS Security Hub	Read			
GetInvitationsCount	Grants permission to retrieve the count of Amazon Macie membership invitations that were received by an account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMacieSession	Grants permission to retrieve information about the status and configuration settings for an Amazon Macie account	Read			
GetMasterAccount	Grants permission to retrieve information about the Amazon Macie administrator account for an account	Read			
GetMember	Grants permission to retrieve information about an account that's associated with an Amazon Macie administrator account	Read	Member*		
GetResourceProfile	Grants permission to retrieve sensitive data discovery statistics and the sensitivity score for an S3 bucket	Read			
GetRevealConfiguration	Grants permission to retrieve the status and configuration settings for retrieving occurrences of sensitive data reported by findings	Read			
GetSensitiveDataOccurrences	Grants permission to retrieve occurrences of sensitive data reported by a finding	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSensitiveDataOccurrencesAvailability	Grants permission to check whether occurrences of sensitive data can be retrieved for a finding	Read			
GetSensitivityInspectionTemplate	Grants permission to retrieve the sensitivity inspection template settings for an account	Read			
GetUsageStatistics	Grants permission to retrieve quotas and aggregated usage data for one or more accounts	Read			
GetUsageTotals	Grants permission to retrieve aggregated usage data for an account	Read			
ListAllowLists	Grants permission to retrieve a subset of information about all the allow lists for an account	List			
ListAutomatedDiscoveryAccounts	Grants permission to retrieve the status of automated sensitive data discovery for an account	List			
ListClassificationJobs	Grants permission to retrieve a subset of information about the status and settings for one or more sensitive data discovery jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClassificationScopes	Grants permission to retrieve a subset of information about the classification scope for an account	List			
ListCustomDataIdentifiers	Grants permission to retrieve information about all custom data identifiers	List			
ListFindings	Grants permission to retrieve a subset of information about one or more findings	List			
ListFindingsFilters	Grants permission to retrieve information about all findings filters	List			
ListInvitations	Grants permission to retrieve information about all the Amazon Macie membership invitations that were received by an account	List			
ListManagedDataIdentifiers	Grants permission to retrieve information about managed data identifiers	List			
ListMembers	Grants permission to retrieve information about the Amazon Macie member accounts that are associated with a Macie administrator account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOrganizationAdminAccounts	Grants permission to retrieve information about the delegated Amazon Macie administrator account for an AWS organization	List			
ListResourceProfileArtifacts	Grants permission to retrieve information about objects that Amazon Macie selected from an S3 bucket for automated sensitive data discovery	List			
ListResourceProfileDetections	Grants permission to retrieve information about the types and amount of sensitive data that Amazon Macie found in an S3 bucket	List			
ListSensitivityInspectionTemplates	Grants permission to retrieve a subset of information about the sensitivity inspection template for an account	List			
ListTagsForResource	Grants permission to retrieve the tags for an Amazon Macie resource	Read	AllowList		
			ClassificationJob		
			CustomDataIdentifier		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			FindingsFilter		
			Member		
PutClassificationExportConfiguration	Grants permission to create or update the settings for storing sensitive data discovery results	Write			
PutFindingsPublicationConfiguration	Grants permission to update the configuration settings for publishing findings to AWS Security Hub	Write			
SearchResources	Grants permission to retrieve statistical data and other information about AWS resources that Amazon Macie monitors and analyzes	Read			
TagResource	Grants permission to add or update the tags for an Amazon Macie resource	Tagging	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
TestCustomDataIdentifier	Grants permission to test a custom data identifier	Write			
UntagResource	Grants permission to remove tags from an Amazon Macie resource	Tagging	AllowList		
			ClassificationJob		
			CustomDataIdentifier		
			FindingsFilter		
			Member		
				aws:TagKeys	
UpdateAllowList	Grants permission to update the settings for an allow list	Write	AllowList*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAutomatedDiscoveryConfiguration	Grants permission to change the status of automated sensitive data discovery for an Amazon Macie administrator account, organization, or standalone account	Write			
UpdateClassificationJob	Grants permission to change the status of a sensitive data discovery job	Write	ClassificationJob*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateClassificationScope	Grants permission to update the classification scope settings for an account	Write			
UpdateFindingsFilter	Grants permission to update the settings for a findings filter	Write	FindingsFilter*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMacieSession	Grants permission to an Amazon Macie administrator account to suspend or re-enable Macie for a member account	Write			
UpdateMemberSession	Grants permission to an Amazon Macie administrator account to suspend or re-enable a Macie member account	Write			
UpdateOrganizationConfiguration	Grants permission to update Amazon Macie configuration settings for an AWS organization	Write			
UpdateResourceProfile	Grants permission to update the sensitivity score for an S3 bucket	Write			
UpdateResourceProfileDetections	Grants permission to update the sensitivity scoring settings for an S3 bucket	Write			
UpdateRevealConfiguration	Grants permission to update the status and configuration settings for retrieving occurrences of sensitive data reported by findings	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSensitivityInspectionTemplate	Grants permission to update the sensitivity inspection template settings for an account	Write			

Resource types defined by Amazon Macie

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
AllowList	`arn:${Partition}:macie2:${Region}:${Account}:allow-list/${ResourceId}`	aws:ResourceTag/${TagKey}
ClassificationJob	`arn:${Partition}:macie2:${Region}:${Account}:classification-job/${ResourceId}`	aws:ResourceTag/${TagKey}
CustomDataIdentifier	`arn:${Partition}:macie2:${Region}:${Account}:custom-data-identifier/${ResourceId}`	aws:ResourceTag/${TagKey}
FindingsFilter	`arn:${Partition}:macie2:${Region}:${Account}:findings-filter/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Member	arn:${Partition}:macie2:${Region}:${Account}:member/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Macie

Amazon Macie defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Mainframe Modernization Application Testing

AWS Mainframe Modernization Application Testing (service prefix: apptest) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Mainframe Modernization Application Testing

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTestCase	Grants permission to create a test case	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestConfiguration	Grants permission to create a test configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTestSuite	Grants permission to create a test suite	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
DeleteTestCase	Grants permission to delete a test case	Write	TestCase*		
DeleteTestConfiguration	Grants permission to delete a test configuration	Write	TestConfiguration*		
DeleteTestRun	Grants permission to delete a test run	Write	TestRun*		s3:DeleteObject s3:ListBucket
DeleteTestSuite	Grants permission to delete a test suite	Write	TestSuite*		
GetTestCase	Grants permission to get a test case	Read	TestCase*		
GetTestConfiguration	Grants permission to get a test configuration	Read	TestConfiguration*		
GetTestRunStep	Grants permission to get test run step	Read	TestRun*		
GetTestSuite	Grants permission to get a test suite	Read	TestSuite*		
ListTagsForResource	Grants permission to list tags for a resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTestCases	Grants permission to list test cases	List			
ListTestConfigurations	Grants permission to list test configurations	List			
ListTestRunSteps	Grants permission to list steps for a test run	Read	TestRun*		
ListTestRunTestCases	Grants permission to list test cases for a test run	Read	TestRun*		
ListTestRuns	Grants permission to list test runs	List			
ListTestSuites	Grants permission to list test suites	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTestRun	Grants permission to start a test run	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:CreateStack cloudformation:DeleteStack cloudformation:DescribeStacks dms:DescribeReplicationTasks dms:StartReplicationTask dms:StopReplicationTask ec2:DescribeAvailabilityZones ec2:DescribeVpcEndpointServ

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iceConfigurations ec2:DescribeVpcEndpointServices m2:CreateDataSetImportTask m2:GetApplication m2:GetApplicationVersion m2:GetBatchJobExecution m2:GetDataSetDetails m2:GetDataSetImportTask m2:StartApplication

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					m2:StartBatchJob m2:StopApplication s3:CreateBucket s3:DeleteObject s3:GetObject s3:ListBucket s3:PutObject
TagResource	Grants permission to tag a resource	Tagging	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	TestCase		
			TestConfiguration		
			TestRun		
			TestSuite		
				aws:TagKeys	
UpdateTestCase	Grants permission to update a test case	Write	TestCase*		
UpdateTestConfiguration	Grants permission to update a test configuration	Write	TestConfiguration*		
UpdateTestSuite	Grants permission to update a test suite	Write	TestSuite*		

Resource types defined by AWS Mainframe Modernization Application Testing

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
TestCase	`arn:${Partition}:apptest:${Region}:${Account}:testcase/${TestCaseId}`	aws:ResourceTag/${TagKey}
TestConfiguration	`arn:${Partition}:apptest:${Region}:${Account}:testconfiguration/${TestConfigurationId}`	aws:ResourceTag/${TagKey}
TestRun	`arn:${Partition}:apptest:${Region}:${Account}:testrun/${TestRunId}`	aws:ResourceTag/${TagKey}
TestSuite	`arn:${Partition}:apptest:${Region}:${Account}:testsuite/${TestSuiteId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Mainframe Modernization Application Testing

AWS Mainframe Modernization Application Testing defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String

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 AWS Mainframe Modernization Service

AWS Mainframe Modernization Service (service prefix: `m2`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Mainframe Modernization Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelBatchJobExecution	Grants permission to cancel the execution of a batch job	Write	Application*		
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject s3:ListBucket
CreateDataSetExportTask	Grants permission to create a data set export task	Write	Application*		s3:GetObject
CreateDataSetImportTask	Grants permission to create a data set import task	Write	Application*		s3:GetObject
CreateDeployment	Grants permission to create a deployment	Write	Application*		elasticloadbalancing:AddTags elasticloadbalancing:CreateListener elasticloadbalancing:Create

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					TargetGroup elasticloadbalancing:RegisterTargets
			Environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironment	Grants permission to Create an environment	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					elasticfilesystem:DescribeMountTargets elasticloadbalancing:AddTags elasticloadbalancing:CreateLoadBalancer fsx:DescribeFileSystems iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplication	Grants permission to delete an application	Write	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteApplicationFromEnvironment	Grants permission to delete an application from a runtime environment	Write	Application*		elasticloadbalancing:DeleteListener elasticloadbalancing:DeleteTargetGroup
DeleteEnvironment	Grants permission to delete a runtime environment	Write	Environment*		elasticloadbalancing:DeleteLoadBalancer
GetApplication	Grants permission to retrieve an application	Read	Application*		
GetApplicationVersion	Grants permission to retrieve an application version	Read	Application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBatchJobExecution	Grants permission to retrieve a batch job execution	Read	Application*		
GetDataSetDetails	Grants permission to retrieve data set details	Read	Application*		
GetDataSetExportTask	Grants permission to export a data set at the specified S3 location	Read	Application*		
GetDataSetImportTask	Grants permission to retrieve a data set import task	Read	Application*		
GetDeployment	Grants permission to retrieve a deployment	Read	Application*		
GetEnvironment	Grants permission to retrieve a runtime environment	Read	Environment*		
GetSignedBluinsightsUrl	Grants permission to create a signed Bluinsights url	Read			
ListApplicationVersions	Grants permission to list the versions of an application	Read	Application*		
ListApplications	Grants permission to list applications	List			
ListBatchJobDefinitions	Grants permission to list batch job definitions	Read	Application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBatchJobExecutions	Grants permission to list executions for a batch job	Read	Application*		
ListBatchJobRestartPoints	Grants permission to retrieve a batch job execution	Read	Application*		
ListDataSetExportHistory	Grants permission to list data set export history	Read	Application*		
ListDataSetImportHistory	Grants permission to list data set import history	Read	Application*		
ListDataSets	Grants permission to list data sets	Read	Application*		
ListDeployments	Grants permission to list deployments	Read	Application*		
ListEngineVersions	Grants permission to list engine versions	Read			
ListEnvironments	Grants permission to list runtime environments	List			
ListTagsForResource	Grants permission to list tags for a resource	Read			
StartApplication	Grants permission to start an application	Write	Application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartBatchJob	Grants permission to start a batch job	Write	Application*		
StopApplication	Grants permission to stop an application	Write	Application*		
TagResource	Grants permission to tag a resource	Tagging	Application		
			Environment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	Application		
			Environment		
				aws:TagKeys	
UpdateApplication	Grants permission to update an application	Write	Application*		s3:GetObject s3:ListBucket

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update a runtime environment	Write	Environment*		

Resource types defined by AWS Mainframe Modernization 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:${Partition}:m2:${Region}:${Account}:app/${ApplicationId}`	aws:ResourceTag/${TagKey}
Environment	`arn:${Partition}:m2:${Region}:${Account}:env/${EnvironmentId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Mainframe Modernization Service

AWS Mainframe Modernization Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${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 Managed Blockchain

Amazon Managed Blockchain (service prefix: `managedblockchain`) 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 Blockchain
- Resource types defined by Amazon Managed Blockchain
- Condition keys for Amazon Managed Blockchain

Actions defined by Amazon Managed Blockchain

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessor	Grants permission to create an Amazon Managed Blockchain accessor	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMember	Grants permission to create a member of an Amazon Managed Blockchain network	Write	network*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNetwork	Grants permission to create an Amazon Managed Blockchain network	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateNode	Grants permission to create a node within a member of an Amazon Managed Blockchain network	Write	member		iam:CreateServiceLinkedRole
			network		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateProposal	Grants permission to create a proposal that other blockchain network members can vote on to add or remove a member in an Amazon Managed Blockchain network	Write	network*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccessor	Grants permission to delete an Amazon Managed Blockchain accessor	Write	accessor*		
DeleteMember	Grants permission to delete a member and all associated resources from an Amazon Managed Blockchain network	Write	member*		
DeleteNode	Grants permission to delete a node from a member of an Amazon Managed Blockchain network	Write	node*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GET [permission only]	Grants permission to send HTTP GET requests to an Ethereum node	Permissions management			
GetAccessor	Grants permission to return detailed information about an Amazon Managed Blockchain accessor	Read	accessor*		
GetMember	Grants permission to return detailed information about a member of an Amazon Managed Blockchain network	Read	member*		
GetNetwork	Grants permission to return detailed information about an Amazon Managed Blockchain network	Read	network*		
GetNode	Grants permission to return detailed information about a node within a member of an Amazon Managed Blockchain network	Read	node*		
GetProposal	Grants permission to return detailed information about a proposal of an Amazon Managed Blockchain network	Read	proposal*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Invoke [permission only]	Grants permission to create WebSocket connections to an Ethereum node	Permissions management			
InvokeRpcBitcoinMainnet	Grants permission to invoke the Bitcoin Mainnet RPCs	Read			
InvokeRpcBitcoinTestnet	Grants permission to invoke the Bitcoin Testnet RPCs	Read			
InvokeRpcPolygonMainnet	Grants permission to invoke the Polygon Mainnet RPCs	Read			
InvokeRpcPolygonMumbaiTestnet	Grants permission to invoke the Polygon Mumbai Testnet RPCs	Read			
ListAccessors	Grants permission to list the Amazon Managed Blockchain accessors owned by the current AWS account	List			
ListInvitations	Grants permission to list the invitations extended to the active AWS account from any Managed Blockchain network	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMembers	Grants permission to list the members of an Amazon Managed Blockchain network and the properties of their memberships	List	network*		
ListNetworks	Grants permission to list the Amazon Managed Blockchain networks in which the current AWS account participates	List			
ListNodes	Grants permission to list the nodes within a member of an Amazon Managed Blockchain network	List	member network		
ListProposalVotes	Grants permission to list all votes for a proposal, including the value of the vote and the unique identifier of the member that cast the vote for the given Amazon Managed Blockchain network	Read	proposal*		
ListProposals	Grants permission to list proposals for the given Amazon Managed Blockchain network	List	network*		
ListTagsForResource	Grants permission to view tags associated with an Amazon Managed Blockchain resource	Read	accessor invitation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			member		
			network		
			node		
			proposal		
POST [permission only]	Grants permission to send HTTP POST requests to an Ethereum node	Permissions management			
RejectInvitation	Grants permission to reject the invitation to join the blockchain network	Write	invitation*		
TagResource	Grants permission to add tags to an Amazon Managed Blockchain resource	Tagging	accessor		
			invitation		
			member		
			network		
			node		
			proposal		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from an Amazon Managed Blockchain resource	Tagging	accessor		
			invitation		
			member		
			network		
			node		
			proposal		
				aws:TagKeys	
UpdateMember	Grants permission to update a member of an Amazon Managed Blockchain network	Write	member*		iam:CreateServiceLinkedRole
UpdateNode	Grants permission to update a node from a member of an Amazon Managed Blockchain network	Write	node*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
VoteOnProposal	Grants permission to cast a vote for a proposal on behalf of the blockchain network member specified	Write	proposal*		

Resource types defined by Amazon Managed Blockchain

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
network	`arn:${Partition}:managedblockchain:${Region}::networks/${NetworkId}`	aws:ResourceTag/${TagKey}
member	`arn:${Partition}:managedblockchain:${Region}:${Account}:members/${MemberId}`	aws:ResourceTag/${TagKey}
node	`arn:${Partition}:managedblockchain:${Region}:${Account}:nodes/${NodeId}`	aws:ResourceTag/${TagKey}
proposal	`arn:${Partition}:managedblockchain:${Region}::proposals/${ProposalId}`	aws:ResourceTag/${TagKey}
invitation	`arn:${Partition}:managedblockchain:${Region}:${Account}:invitations/${InvitationId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
accessor	arn:${Partition}:managedblockchain:${Region}:${Account}:accessors/${AccessorId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Managed Blockchain

Amazon Managed Blockchain defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on the tags associated with an Amazon Managed Blockchain resource	String
aws:TagKeys	Filters actions based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Managed Blockchain Query

Amazon Managed Blockchain Query (service prefix: managedblockchain-query) 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 Blockchain Query

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetTokenBalance	Grants permission to batch calls for GetTokenBalance API	Read			
GetAssetContract	Grants permission to fetch information about a contract on the blockchain	Read			
GetTokenBalance	Grants permission to retrieve balance of a token for an address on the blockchain	Read			
GetTransaction	Grants permission to retrieve a transaction on the blockchain	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssetContracts	Grants permission to fetch multiple contracts on the blockchain	List			
ListFilteredTransactionEvents	Grants permission to retrieve events on the blockchain with additional filters	List			
ListTokenBalances	Grants permission to retrieve multiple balances on the blockchain	List			
ListTransactionEvents	Grants permission to retrieve events in a transaction on the blockchain	List			
ListTransactions	Grants permission to retrieve a multiple transactions on a blockchain	List			

Resource types defined by Amazon Managed Blockchain Query

Amazon Managed Blockchain Query does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Managed Blockchain Query, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Managed Blockchain Query

Managed Blockchain Query has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Managed Grafana

Amazon Managed Grafana (service prefix: `grafana`) 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 Grafana

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateLicense	Grants permission to upgrade a workspace with a license	Write	workspace*		aws-marketplace:ViewSubscriptions
CreateWorkspace	Grants permission to create a workspace	Write		aws:TagKeys	ec2:DescribeSecurityGroups

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole organizations:DescribeOrganization sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions sso:GetSharedSsoConfiguration

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkspaceApiKey	Grants permission to create API keys for a workspace	Write	workspace*		
CreateWorkspaceServiceAccount	Grants permission to create service accounts for a workspace	Write	workspace*		
CreateWorkspaceServiceAccountToken	Grants permission to create service account tokens for a workspace	Write	workspace*		
DeleteWorkspace	Grants permission to delete a workspace	Write	workspace*		sso:DeleteManagedApplicationInstance
DeleteWorkspaceApiKey	Grants permission to delete API keys from a workspace	Write	workspace*		
DeleteWorkspaceServiceAccount	Grants permission to delete service accounts for a workspace	Write	workspace*		
DeleteWorkspaceServiceAccountToken	Grants permission to delete service account tokens for a workspace	Write	workspace*		
DescribeWorkspace	Grants permission to describe a workspace	Read	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWorkspaceAuthentication	Grants permission to describe authentication providers on a workspace	Read	workspace*		
DescribeWorkspaceConfiguration	Grants permission to describe the current configuration string for the given workspace	Read	workspace*		
DisassociateLicense	Grants permission to remove a license from a workspace	Write	workspace*		
ListPermissions	Grants permission to list the permissions on a wokspace	List	workspace*		
ListTagsForResource	Grants permission to list tags associated with a workspace	Read	workspace		
ListVersions	Grants permission to list all available supported Grafana versions. Optionally, include a workspace to list the versions to which it can be upgraded	List	workspace		
ListWorkspaceServiceAccountTokens	Grants permission to list service account tokens for a workspace	Read	workspace*		
ListWorkspaceServiceAccounts	Grants permission to list service accounts for a workspace	Read	workspace*		
ListWorkspaces	Grants permission to list workspaces	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to, or update tag values of, a workspace	Tagging	workspace*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a workspace	Tagging	workspace*		
				aws:TagKeys	
UpdatePermissions	Grants permission to modify the permissions on a workspace	Permissions management	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWorkspace	Grants permission to modify a workspace	Write	workspace*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:GetManagedPrefixListEntries iam:CreateServiceLinkedRole
UpdateWorkspaceAuthentication	Grants permission to modify authentication providers on a workspace	Write	workspace*		
UpdateWorkspaceConfiguration	Grants permission to update the configuration string for the given workspace	Write	workspace*		

Resource types defined by Amazon Managed Grafana

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:${Partition}:grafana:${Region}:${Account}:/workspaces/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Managed Grafana

Amazon Managed Grafana defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus (service prefix: aps) 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 Service for Prometheus

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAlertManagerAlerts	Grants permission to create alerts	Write	workspace*		
				aws:ResourceTag/${TagKey}	
CreateAlertManagerDefinition	Grants permission to create an alert manager definition	Write	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAnomalyDetector	Grants permission to create an anomaly detector	Write	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggingConfiguration	Grants permission to create a logging configuration	Write	workspace*		
				aws:ResourceTag/${TagKey}	
CreateQueryLoggingConfiguration	Grants permission to create a query logging configuration	Write	workspace*		
				aws:ResourceTag/${TagKey}	
CreateRuleGroupsNamespace	Grants permission to create a rule groups namespace	Write	rulegroupsnamespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScraper	Grants permission to create a scraper	Write	cluster*		aps:TagResource ec2:DescribeSecurityGroups ec2:DescribeSubnets eks:DescribeCluster iam:CreateServiceLinkedRole
			workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateWorkspace	Grants permission to create a workspace	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlertManagerDefinition	Grants permission to delete an alert manager definition	Write	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteAlertManagerSilence	Grants permission to delete a silence	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteAnomalyDetector	Grants permission to delete an anomaly detector	Write	anomalydetector*		
			workspace*		
				aws:ResourceTag/${TagKey}	
DeleteLoggingConfiguration	Grants permission to delete a logging configuration	Write	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteQueryLoggingConfiguration	Grants permission to delete a query logging configuration	Write	workspace*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Grants permission to delete workspace resource policy	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteRuleGroupsNamespace	Grants permission to delete a rule groups namespace	Write	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DeleteScraper	Grants permission to delete a scraper	Write	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteScraperLoggingConfiguration	Grants permission to delete a scraper logging configuration	Write	scraper*		
				aws:ResourceTag/${TagKey}	
DeleteWorkspace	Grants permission to delete a workspace	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DescribeAlertManagerDefinition	Grants permission to describe an alert manager definition	Read	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeAnomalyDetector	Grants permission to describe an anomaly detector	Read	anomalydetector*		
			workspace*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingConfiguration	Grants permission to describe a logging configuration	Read	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeQueryLoggingConfiguration	Grants permission to describe a query logging configuration	Read	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeResourcePolicy	Grants permission to describe workspace resource policy	Read	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeRuleGroupsNamespace	Grants permission to describe a rule groups namespace	Read	rulegroupsnamespace*		
				aws:ResourceTag/${TagKey}	
DescribeScraper	Grants permission to describe a scraper	Read	scraper*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScraperLoggingConfiguration	Grants permission to describe a scraper logging configuration	Read	scraper*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspace	Grants permission to describe a workspace	Read	workspace*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceConfiguration	Grants permission to describe workspace configuration	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerSilence	Grants permission to get a silence	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetAlertManagerStatus	Grants permission to get current status of an alertmanager	Read	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetDefaultScraperConfiguration	Grants permission to get default scraper configuration	Read			
GetLabels	Grants permission to retrieve AMP workspace labels	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetMetricMetadata	Grants permission to retrieve the metadata for AMP workspace metrics	Read	workspace*		
				aws:ResourceTag/${TagKey}	
GetSeries	Grants permission to retrieve AMP workspace time series data	Read	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAlertManagerAlertGroups	Grants permission to list groups	Read	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerAlerts	Grants permission to list alerts	Read	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerReceivers	Grants permission to list receivers	Read	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlertManagerSilences	Grants permission to list silences	Read	workspace*		
				aws:ResourceTag/${TagKey}	
ListAlerts	Grants permission to list active alerts	Read	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListAnomalyDetectors	Grants permission to list anomaly detectors	List	workspace*		
				aws:ResourceTag/${TagKey}	
ListRuleGroupsNamespaces	Grants permission to list rule groups namespaces	List	workspace*		
				aws:ResourceTag/${TagKey}	
ListRules	Grants permission to list alerting and recording rules	Read	workspace*		
				aws:ResourceTag/${TagKey}	
ListScrapers	Grants permission to list scrapers	List			
ListTagsForResource	Grants permission to list tags on an AMP resource	Read	anomalydetector		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListWorkspaces	Grants permission to list workspaces	List			
PreviewAnomalyDetector	Grants permission to preview anomaly detection on AMP workspace metrics	Read	workspace*		
				aws:ResourceTag/${TagKey}	
PutAlertManagerDefinition	Grants permission to update an alert manager definition	Write	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAlertManagerSilences	Grants permission to create or update a silence	Write	workspace*		
				aws:ResourceTag/${TagKey}	
PutAnomalyDetector	Grants permission to update an anomaly detector	Write	anomalydetector*		
			workspace*		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy	Grants permission to create and update workspace resource policy	Write	workspace*		
				aws:ResourceTag/${TagKey}	
PutRuleGroupsNamespace	Grants permission to update a rule groups namespace	Write	rulegroupsnamespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
QueryMetrics	Grants permission to run a query on AMP workspace metrics	Read	workspace*		
				aws:ResourceTag/${TagKey}	
RemoteWrite	Grants permission to perform a remote write operation to initiate the streaming of metrics to AMP workspace	Write	workspace*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag an AMP resource	Tagging	anomalydetector		
			rulegroupsnamespace		
			scraper		
			workspace		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag an AMP resource	Tagging	anomalydetector		
			rulegroupsnamespace		
			scraper		
			workspace		
				aws:TagKeys	
UpdateLoggingConfiguration	Grants permission to update a logging configuration	Write	workspace*		
				aws:ResourceTag/${TagKey}	
UpdateQueryLoggingConfiguration	Grants permission to update a query logging configuration	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateScraper	Grants permission to update a scraper	Write	scraper*		aps:CreateScraper aps:TagResource
			workspace		
				aws:ResourceTag/${TagKey}	
UpdateScraperLoggingConfiguration	Grants permission to put a scraper logging configuration	Write	scraper*		
				aws:ResourceTag/${TagKey}	
UpdateWorkspaceAlias	Grants permission to modify the alias of existing AMP workspace	Write	workspace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWorkspaceConfiguration	Grants permission to update workspace configuration	Write	workspace *		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Managed Service for Prometheus

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:${Partition}:aps:${Region}:${Account}:workspace/${WorkspaceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
rulegroupsnamespace	`arn:${Partition}:aps:${Region}:${Account}:rulegroupsnamespace/${WorkspaceId}/${Namespace}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		aws:TagKeys
anomalydetector	arn:${Partition}:aps:${Region}:${Account}:anomalydetector/${WorkspaceId}/${AnomalyDetectorId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
scraper	arn:${Partition}:aps:${Region}:${Account}:scraper/${ScraperId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
cluster	arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka (service prefix: `kafka`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Managed Streaming for Apache Kafka
- Resource types defined by Amazon Managed Streaming for Apache Kafka
- Condition keys for Amazon Managed Streaming for Apache Kafka

Actions defined by Amazon Managed Streaming for Apache Kafka

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAssociateScramSecret	Grants permission to associate one or more Scram Secrets with an Amazon MSK cluster	Write	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Grants permission to disassociate one or more Scram Secrets from an Amazon MSK cluster	Write	cluster*		kms:RetireGrant
CreateCluster	Grants permission to create an MSK cluster	Write	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					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	
CreateTopic	Grants permission to create a Kafka topic in an MSK cluster	Write	topic*		kafka-cluster:Connect kafka-cluster:CreateTopic

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*		
DeleteTopic	Grants permission to delete a Kafka topic from an MSK cluster	Write	topic*		kafka-cluster:Connect kafka-cluster:DeleteTopic kafka-cluster:DescribeTopic
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribeTopic	Grants permission to return metadata details about a specific Kafka topic	Read	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic kafka-cluster:DescribeTopicDynamicConfiguration

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTopicPartitions	Grants permission to list all partitions of a specific topic	Read	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic kafka-cluster:DescribeTopicDynamicConfiguration
DescribeVpcConnection	Grants permission to describe a MSK VPC connection	Read	vpc-connection*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClientVpcConnections	Grants permission to list all MSK VPC connections created for a cluster	List	cluster*		
ListClusterOperations	Grants permission to return a list of all the operations that have been performed on the specified MSK cluster	List	cluster*		
ListClusterOperationsV2	Grants permission to return a list of all the operations that have been performed on the specified MSK cluster	List	cluster*		
ListClusters	Grants permission to list all MSK clusters in this account	List			
ListClustersV2	Grants permission to list all MSK clusters in this account	List			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListReplicators	Grants permission to list all MSK replicators in this account	List			
ListScramSecrets	Grants permission to list the Scram Secrets associated with an Amazon MSK cluster	List	cluster*		
ListTagsForResource	Grants permission to list tags of an MSK resource	Read	cluster*		
ListTopics	Grants permission to list all Kafka topics for a specified MSK cluster	List	cluster*		kafka-cluster:Connect kafka-cluster:DescribeTopic
ListVpcConnections	Grants permission to list all MSK VPC connections that this account uses	List			
PutClusterPolicy	Grants permission to create or update the resource-based policy for a cluster	Write	cluster*		
RebootBroker	Grants permission to reboot broker	Write	cluster*		
RejectClientVpcConnection	Grants permission to reject a MSK VPC connection	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRebalancing	Grants permission to update the intelligent rebalancing status of the MSK cluster	Write	cluster*		
UpdateReplicationInfo	Grants permission to update the replication info of the MSK replicator	Write	replicator*		
UpdateSecurity	Grants permission to update the security settings for the MSK cluster	Write	cluster*		kms:RetireGrant
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTopic	Grants permission to update the configuration of a Kafka topic in an MSK cluster	Write	topic*		kafka-cluster:AlterTopic kafka-cluster:AlterTopicDynamicConfiguration kafka-cluster:Connect kafka-cluster:DescribeTopic

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}

Resource types	ARN	Condition keys
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}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Condition keys for Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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 Streaming for Kafka Connect

Amazon Managed Streaming for Kafka Connect (service prefix: `kafkaconnect`) 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 Kafka Connect
- Resource types defined by Amazon Managed Streaming for Kafka Connect
- Condition keys for Amazon Managed Streaming for Kafka Connect

Actions defined by Amazon Managed Streaming for Kafka 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 AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnector	Grants permission to create an MSK Connect connector	Write			ec2:CreateNetworkInterface ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs firehose:TagDeliveryStream iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					logs:CreateLogDelivery logs:DescribeLogGroups logs:DescribeResourcePolicies logs:GetLogDelivery logs:ListLogDeliveries logs:PutResourcePolicy s3:GetBucketPolicy s3:PutBucketPolicy
CreateCustomPlugin	Grants permission to create an MSK Connect custom plugin	Write			s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkerConfiguration	Grants permission to create an MSK Connect worker configuration	Write			
DeleteConnector	Grants permission to delete an MSK Connect connector	Write	connector*		logs:DeleteLogDelivery logs:ListLogDeliveries
DeleteCustomPlugin	Grants permission to delete an MSK Connect custom plugin	Write	custom plugin*		
DeleteWorkerConfiguration	Grants permission to delete an MSK Connect worker configuration	Write	worker configuration*		
DescribeConnector	Grants permission to describe an MSK Connect connector	Read	connector*		
DescribeConnectorOperation	Grants permission to describe a MSK Connect connector operation	Read	connector operation*		
DescribeCustomPlugin	Grants permission to describe an MSK Connect custom plugin	Read	custom plugin*		
DescribeWorkerConfiguration	Grants permission to describe an MSK Connect worker configuration	Read	worker configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConnectorOperations	Grants permission to list all operations of a given MSK Connect connector	Read	connector *		
ListConnectors	Grants permission to list all MSK Connect connectors in this account	Read			
ListCustomPlugins	Grants permission to list all MSK Connect custom plugins in this account	Read			
ListTagsForResource	Grants permission to list tags of an MSK Connect resource	Read	connector	aws:ResourceTag/${TagKey}	
			custom plugin	aws:ResourceTag/${TagKey}	
			worker configuration	aws:ResourceTag/${TagKey}	
ListWorkerConfigurations	Grants permission to list all MSK Connect worker configurations in this account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an MSK Connect resource	Tagging	connector	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			custom plugin	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			worker configuration	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from an MSK Connect resource	Tagging	connector	aws:TagKeys	
			custom plugin	aws:TagKeys	
			worker configuration	aws:TagKeys	
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnector	Grants permission to update an MSK Connect connector	Write	connector *		

Resource types defined by Amazon Managed Streaming for Kafka 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
connector	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector/${ConnectorName}/${UUID}`	aws:ResourceTag/${TagKey}
custom plugin	`arn:${Partition}:kafkaconnect:${Region}:${Account}:custom-plugin/${CustomPluginName}/${UUID}`	aws:ResourceTag/${TagKey}
worker configuration	`arn:${Partition}:kafkaconnect:${Region}:${Account}:worker-configuration/${WorkerConfigurationName}/${UUID}`	aws:ResourceTag/${TagKey}
connector operation	`arn:${Partition}:kafkaconnect:${Region}:${Account}:connector-operation/${ConnectorName}/${ConnectorUUID}/${UUID}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Managed Streaming for Kafka Connect

Amazon Managed Streaming for Kafka 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
CreateWebLoginToken	Grants permission to create a short-lived token that allows a user to log into Apache Airflow web UI	Write	rbac-role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Grants permission to modify an Amazon MWAA environment	Write	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}`	
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Marketplace

AWS 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 AWS Marketplace
- Resource types defined by AWS Marketplace
- Condition keys for AWS Marketplace

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAgreementApprovalRequest	Grants permission to users to approve an incoming subscription request (for providers who provide products that require subscription verification)	Write			
AcceptAgreementPaymentRequest	Grants permission to users to accept a payment request	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			
CancelAgreementPaymentRequest	Grants permission to users to cancel a payment request	Write			
CancelAgreementRequest	Grants permission to users to cancel pending subscription requests for products that require subscription verification	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetAgreementPaymentRequest	Grants permission to users to view details for a payment request	Read			
GetAgreementRequest	Grants permission to users to view the details of their subscription requests for data products that require subscription verification	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAgreementTerms	Grants permission to users to get a list of terms for an agreement	List			
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			
ListAgreementPaymentRequests	Grants permission to users to list payment requests for an agreement	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectAgreementApprovalRequest	Grants permission to users to decline an incoming subscription requests (for providers who provide products that require subscription verification)	Write			
RejectAgreementPaymentRequest	Grants permission to users to reject a payment request	Write			
SearchAgreements	Grants permission to users to search their agreements	List			
SendAgreementPaymentRequest	Grants permission to users to send payment request	Write			
Subscribe	Grants permission to users to subscribe to AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Unsubscribe	Grants permission to users to remove subscriptions to AWS 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			
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 AWS Marketplace

AWS Marketplace does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace

AWS 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 AWS 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
aws-marketplace:ProductId	Filters access by product id for AWS Marketplace RedHat OpenShift and Bedrock Products. Note: Using this condition key will not restrict access to products in AWS Marketplace	ArrayOfString

Actions, resources, and condition keys for AWS Marketplace Catalog

AWS Marketplace Catalog (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Catalog

- Resource types defined by AWS Marketplace Catalog
- Condition keys for AWS Marketplace Catalog

Actions defined by AWS Marketplace Catalog

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelChangeSet	Grants permission to cancel a running change set	Write	ChangeSet*		
DeleteResourcePolicy	Grants permission to delete the resource policy of an existing entity	Permissions management	Entity*		
DescribeAssessment	Grants permission to return the details of an existing assessment	Read	Assessment		
DescribeChangeSet	Grants permission to return the details of an existing change set	Read	ChangeSet*		
DescribeEntity	Grants permission to return the details of an existing entity	Read	Entity*		
GetResourcePolicy	Grants permission to get the resource policy of an existing entity	Read	Entity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssessments	Grants permission to list existing assessments	List			
ListChangeSets	Grants permission to list existing change sets	List			
ListEntities	Grants permission to list existing entities	List			
ListTagsForResource	Grants permission to list tags on an existing entity or a change set	Read	ChangeSet		
			Entity		
PutResourcePolicy	Grants permission to attach a resource policy to an existing entity	Permissions management	Entity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartChangeSet	Grants permission to request a new change set (Note: resource-level permissions for this action and condition context keys for this action are only supported when used with Catalog API and are not supported when used with AWS Marketplace Management Portal)	Write	Entity*		
				catalog:ChangeType aws-marketplace:Intent aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to tag an existing entity or a change set	Tagging	ChangeSet		
			Entity		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag an existing entity or a change set	Tagging	ChangeSet		
			Entity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	

Resource types defined by AWS Marketplace Catalog

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
Entity	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/${EntityType}/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType
ChangeSet	`arn:${Partition}:aws-marketplace:${Region}:${Account}:${Catalog}/ChangeSet/${ResourceId}`	aws:ResourceTag/${TagKey} catalog:ChangeType
Assessment	`arn:${Partition}:aws-marketplace:${Region}::${Catalog}/Assessment/${ResourceId}`	

Condition keys for AWS Marketplace Catalog

AWS Marketplace Catalog defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the

policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws-marketplace:Intent	Filters access by the Intent parameter in the StartChangeSet 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
catalog:ChangeType	Filters access by the change type in the StartChangeSet request	String

Actions, resources, and condition keys for AWS Marketplace Commerce Analytics Service

AWS Marketplace Commerce Analytics Service (service prefix: `marketplacecommerceanalytics`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.

Topics

- Actions defined by AWS Marketplace Commerce Analytics Service

- Resource types defined by AWS Marketplace Commerce Analytics Service
- Condition keys for AWS Marketplace Commerce Analytics Service

Actions defined by AWS Marketplace Commerce Analytics Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataSet	Request a data set to be published to your Amazon S3 bucket.	Write			
StartSupportDataExport	Request a support data set to be published to your Amazon S3 bucket.	Write			

Resource types defined by AWS Marketplace Commerce Analytics Service

AWS Marketplace Commerce Analytics Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Commerce Analytics Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Commerce Analytics Service

CAS has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Deployment Service

AWS Marketplace Deployment Service (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Marketplace Deployment Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a deployment parameter resource	Read	DeploymentParameter		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDeploymentParameter	Grants permission to create or update a deployment parameter resource	Write	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	aws-marketplace:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a deployment parameter resource	Tagging	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a deployment parameter resource	Tagging	DeploymentParameter*	aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	

Resource types defined by AWS Marketplace Deployment 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
DeploymentParameter	`arn:${Partition}:aws-marketplace:${Region}:${Account}:DeploymentParameter:catalogs/${CatalogName}/products/${ProductId}/${ResourceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Condition keys for AWS Marketplace Deployment Service

AWS Marketplace Deployment Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Marketplace Discovery

AWS Marketplace Discovery (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Discovery
- Resource types defined by AWS Marketplace Discovery
- Condition keys for AWS Marketplace Discovery

Actions defined by AWS Marketplace Discovery

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrivateListings	Grants permission to users to list their private offers	List			

Resource types defined by AWS Marketplace Discovery

AWS Marketplace Discovery does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Discovery, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Discovery

Marketplace Discovery has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Entitlement Service

AWS Marketplace Entitlement Service (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Entitlement Service
- Resource types defined by AWS Marketplace Entitlement Service
- Condition keys for AWS Marketplace Entitlement Service

Actions defined by AWS Marketplace Entitlement Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEntitlements	Grants permission to retrieve entitlement values for a given product. The results can be filtered based on customer identifier or product dimensions	Read			

Resource types defined by AWS Marketplace Entitlement Service

AWS Marketplace Entitlement Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Entitlement Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Entitlement Service

Marketplace Entitlement has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Image Building Service

AWS Marketplace Image Building Service (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Marketplace Image Building Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBuilds [permission only]	Describes Image Builds identified by a build Id	Read			
ListBuilds [permission only]	Lists Image Builds.	Read			
StartBuild [permission only]	Starts an Image Build	Write			

Resource types defined by AWS Marketplace Image Building Service

AWS Marketplace Image Building Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Image Building Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Image Building Service

Marketplace Image Build has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Management Portal

AWS 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 AWS Marketplace Management Portal
- Resource types defined by AWS Marketplace Management Portal
- Condition keys for AWS Marketplace Management Portal

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Marketplace Management Portal	Write			
viewMarketing [permission only]	Allows access to the Marketing page inside the AWS Marketplace Management Portal	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
viewReports [permission only]	Allows access to the Reports page inside the AWS Marketplace Management Portal	List			
viewSettings [permission only]	Allows access to the Settings page inside the AWS Marketplace Management Portal	List			
viewSupport [permission only]	Allows access to the Customer Support Eligibility page inside the AWS Marketplace Management Portal	List			

Resource types defined by AWS Marketplace Management Portal

AWS Marketplace Management Portal does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Management Portal, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Metering Service

AWS Marketplace Metering Service (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Marketplace Metering Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchMeterUsage	Grants permission to post metering records for a set of customers for SaaS applications	Write			
MeterUsage	Grants permission to emit metering records	Write			
RegisterUsage	Grants permission to to verify that the customer running your paid software is subscribed to your product on AWS Marketplace,	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	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 AWS Marketplace Metering Service

AWS Marketplace Metering Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Metering Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Metering Service

Marketplace Metering has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Private Marketplace

AWS Marketplace Private 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 AWS Marketplace Private 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateProductsWithPrivateMarketplace [permission only]	Grants permission to approve a request for a product to be associated with the Private Marketplace. This action can be performed by any account in an AWS Organization, provided the user has permissions to do so, and the Organization's Service Control Policies allow it	Write			
CreatePrivateMarketplaceRequests [permission only]	Grants permission to create a new request for a product or products to be associated with the Private Marketplace. This action can be performed by any account in an in an AWS Organization, provided the user has permissions to	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	do so, and the Organization's Service Control Policies allow it				
DescribePrivateMarketplaceRequests [permission only]	Grants permission to describe requests and associated products in the Private Marketplace. This action can be performed by any account in an AWS Organization, provided the user has permissions to do so, and the Organization's Service Control Policies allow it	List			
DisassociateProductsFromPrivateMarketplace [permission only]	Grants permission to decline a request for a product to be associated with the Private Marketplace. This action can be performed by any account in an AWS Organization, provided the user has permissions to do so, and the Organization's Service Control Policies allow it	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrivateMarketplaceRequests [permission only]	Grants permission to get a queryable list for requests and associated products in the Private Marketplace. This action can be performed by any account in an AWS Organization, provided the user has permissions to do so, and the Organization's Service Control Policies allow it	List			

Resource types defined by AWS Marketplace Private Marketplace

AWS Marketplace Private Marketplace does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Private Marketplace, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Private Marketplace

Private Marketplace has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Procurement Systems Integration

AWS Marketplace Procurement Systems Integration (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Marketplace Procurement Systems Integration

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProcurementSystemConfiguration [permission only]	Grants permission to describe the Procurement System integration configuration (e.g. Coupa) for the individual account, or for the entire AWS Organization if one exists. This action can only be performed by the master account if using an AWS Organization	Read			
PutProcurementSystemConfiguration [permission only]	Grants permission to create or update the Procurement System integration configuration (e.g. Coupa) for the individual account, or for the entire AWS Organization if	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	one exists. This action can only be performed by the master account if using an AWS Organization				

Resource types defined by AWS Marketplace Procurement Systems Integration

AWS Marketplace Procurement Systems Integration does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Procurement Systems Integration, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Procurement Systems Integration

Marketplace Procurement Integration has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Reporting

AWS Marketplace Reporting (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Reporting
- Resource types defined by AWS Marketplace Reporting
- Condition keys for AWS Marketplace Reporting

Actions defined by AWS Marketplace Reporting

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBuyerDashboard	Grants permission to view a dashboard that shows a buyer's AWS Marketplace purchase data	Read	Dashboard *		

Resource types defined by AWS Marketplace Reporting

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
Dashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Condition keys for AWS Marketplace Reporting

Marketplace Reporting has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Seller Reporting

AWS Marketplace Seller Reporting (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Seller Reporting
- Resource types defined by AWS Marketplace Seller Reporting
- Condition keys for AWS Marketplace Seller Reporting

Actions defined by AWS Marketplace Seller Reporting

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSellerDashboard	Grants permission to view a seller dashboard	Read	SellerDashboard*		

Resource types defined by AWS Marketplace Seller Reporting

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
SellerDashboard	`arn:${Partition}:aws-marketplace::${Account}:${Catalog}/ReportingData/${FactTable}/Dashboard/${DashboardName}`	

Condition keys for AWS Marketplace Seller Reporting

Marketplace Seller Reporting has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights (service prefix: `vendor-insights`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Vendor Insights

- Resource types defined by AWS Marketplace Vendor Insights
- Condition keys for AWS Marketplace Vendor Insights

Actions defined by AWS Marketplace Vendor Insights

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateSecurityProfile	Grants permission to activate the security profile	Write	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
AssociateDataSource	Grants permission to associate security profile with a data source	Write	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
CreateDataSource	Grants permission to create a new data source	Write		aws:ResourceTag/${TagKey}	vendor-insights:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSecurityProfile	Grants permission to create a new security profile	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	vendor-insights:TagResource
DeactivateSecurityProfile	Grants permission to deactivate the security profile	Write	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Grants permission to delete a data source	Write	DataSource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DisassociateDataSource	Grants permission to disassociate security profile from a data source	Write	SecurityProfile*		vendor-insights:GetDataSource
				aws:ResourceTag/${TagKey}	
GetDataSource	Grants permission to retrieve the details of an existing data source	Read	DataSource*		
				aws:ResourceTag/${TagKey}	
GetEntitledSecurityProfileSnapshot	Grants permission to return the details of a security profile snapshot that requester is entitled to read	Read	SecurityProfile*		
GetProfileAccessTerms	Grants permission to get the access terms for a vendor insights profile	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSecurityProfile	Grants permission to return the details of an existing security profile	Read	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
GetSecurityProfileSnapshot	Grants permission to return the details of a security profile snapshot	Read	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
ListDataSources	Grants permission to list existing data sources	List			
ListEntitledSecurityProfileSnapshots	Grants permission to return the snapshot summary list for an existing security profile that requester is entitled to list	List	SecurityProfile*		
ListEntitledSecurityProfiles	Grants permission to list entitled security profiles	List			
ListSecurityProfileSnapshots	Grants permission to return the snapshot summary list for an existing security profile	List	SecurityProfile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListSecurityProfiles	Grants permission to list existing security profiles	List			
ListTagsForResource	Grants permission to list tags for vendor insights resource	Read	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag vendor insights resource	Tagging	DataSource		
			SecurityProfile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag vendor insights resource	Tagging	DataSource		
			SecurityProfile		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDataSource	Grants permission to update an existing data source	Write	DataSource*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecurityProfile	Grants permission to update the security profile	Write	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotCreationConfiguration	Grants permission to update the security profile snapshot creation configuration	Write	SecurityProfile*		
				aws:ResourceTag/${TagKey}	
UpdateSecurityProfileSnapshotReleaseConfiguration	Grants permission to update the security profile snapshot release configuration	Write	SecurityProfile*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS Marketplace Vendor 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
DataSource	arn:${Partition}:vendor-insights:::data-source:${ResourceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
SecurityProfile	arn:${Partition}:vendor-insights:::security-profile:${ResourceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Condition keys for AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS MCP Server

AWS MCP Server (service prefix: `aws-mcp`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS MCP Server
- Resource types defined by AWS MCP Server
- Condition keys for AWS MCP Server

Actions defined by AWS MCP Server

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CallReadOnlyTool	Grants permission to call read-only tools in MCP service	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CallReadWriteTool	Grants permission to call AWS Read and Write apis in MCP Service	Write			
InvokeMcp	Grants permission to use MCP service	List			

Resource types defined by AWS MCP Server

AWS MCP Server does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS MCP Server, specify `"Resource": "*"` in your policy.

Condition keys for AWS MCP Server

AWS MCP has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Mechanical Turk

Amazon Mechanical Turk (service prefix: `mechanicalturk`) 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 Mechanical Turk
- Resource types defined by Amazon Mechanical Turk

- Condition keys for Amazon Mechanical Turk

Actions defined by Amazon Mechanical Turk

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptQualificationRequest	The AcceptQualificationRequest operation grants a Worker's request for a Qualification	Write			
ApproveAssignment	The ApproveAssignment operation approves the results of a completed assignment	Write			
AssociateQualificationWithWorker	The AssociateQualificationWithWorker operation gives a Worker a Qualification	Write			
CreateAdditionalAssignmentsForHIT	The CreateAdditionalAssignmentsForHIT operation increases the maximum number of assignments of an existing HIT	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHIT	The CreateHIT operation creates a new HIT (Human Intelligence Task)	Write			
CreateHITType	The CreateHITType operation creates a new HIT type	Write			
CreateHITWithHITType	The CreateHITWithHITType operation creates a new Human Intelligence Task (HIT) using an existing HITTypeID generated by the CreateHITType operation	Write			
CreateQualificationType	The CreateQualificationType operation creates a new Qualification type, which is represented by a QualificationType data structure	Write			
CreateWorkerBlock	The CreateWorkerBlock operation allows you to prevent a Worker from working on your HITs	Write			
DeleteHIT	The DeleteHIT operation disposes of a HIT that is no longer needed	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteQualificationType	The DeleteQualificationType disposes a Qualification type and disposes any HIT types that are associated with the Qualification type	Write			
DeleteWorkerBlock	The DeleteWorkerBlock operation allows you to reinstate a blocked Worker to work on your HITs	Write			
DisassociateQualificationFromWorker	The DisassociateQualificationFromWorker revokes a previously granted Qualification from a user	Write			
GetAccountBalance	The GetAccountBalance operation retrieves the amount of money in your Amazon Mechanical Turk account	Read			
GetAssignment	The GetAssignment retrieves an assignment with an AssignmentStatus value of Submitted, Approved, or Rejected, using the assignment's ID	Read			
GetFileUploadURL	The GetFileUploadURL operation generates and returns a temporary URL	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHIT	The GetHIT operation retrieves the details of the specified HIT	Read			
GetQualificationScore	The GetQualificationScore operation returns the value of a Worker's Qualification for a given Qualification type	Read			
GetQualificationType	The GetQualificationType operation retrieves information about a Qualification type using its ID	Read			
ListAssignmentsForHIT	The ListAssignmentsForHIT operation retrieves completed assignments for a HIT	List			
ListBonusPayments	The ListBonusPayments operation retrieves the amounts of bonuses you have paid to Workers for a given HIT or assignment	List			
ListHITs	The ListHITs operation returns all of a Requester's HITs	List			
ListHITsForQualificationType	The ListHITsForQualificationType operation returns the HITs that use the given QualififcationType for a QualificationRequirement	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListQualificationRequests	The ListQualificationRequests operation retrieves requests for Qualifications of a particular Qualification type	List			
ListQualificationTypes	The ListQualificationTypes operation searches for Qualification types using the specified search query, and returns a list of Qualification types	List			
ListReviewPolicyResultsForHIT	The ListReviewPolicyResultsForHIT operation retrieves the computed results and the actions taken in the course of executing your Review Policies during a CreateHIT operation	List			
ListReviewableHITs	The ListReviewableHITs operation returns all of a Requester's HITs that have not been approved or rejected	List			
ListWorkerBlocks	The ListWorkersBlocks operation retrieves a list of Workers who are blocked from working on your HITs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkersWithQualificationType	The ListWorkersWithQualificationType operation returns all of the Workers with a given Qualification type	List			
NotifyWorkers	The NotifyWorkers operation sends an email to one or more Workers that you specify with the Worker ID	Write			
RejectAssignment	The RejectAssignment operation rejects the results of a completed assignment	Write			
RejectQualificationRequest	The RejectQualificationRequest operation rejects a user's request for a Qualification	Write			
SendBonus	The SendBonus operation issues a payment of money from your account to a Worker	Write			
SendTestEventNotification	The SendTestEventNotification operation causes Amazon Mechanical Turk to send a notification message as if a HIT event occurred, according to the provided notification specification	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExpirationForHIT	The UpdateExpirationForHIT operation allows you extend the expiration time of a HIT beyond is current expiration or expire a HIT immediately	Write			
UpdateHITReviewStatus	The UpdateHITReviewStatus operation toggles the status of a HIT	Write			
UpdateHITTypeOfHIT	The UpdateHITTypeOfHIT operation allows you to change the HITType properties of a HIT	Write			
UpdateNotificationSettings	The UpdateNotificationSettings operation creates, updates, disables or re-enables notifications for a HIT type	Write			
UpdateQualificationType	The UpdateQualificationType operation modifies the attributes of an existing Qualification type, which is represented by a QualificationType data structure	Write			

Resource types defined by Amazon Mechanical Turk

Amazon Mechanical Turk does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Mechanical Turk, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Mechanical Turk

MechanicalTurk has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

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 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/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
CopySnapshot	Grants permissions to make a copy of an existing snapshot	Write	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	Grants permissions to create a new access control list	Write	user*		memorydb:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PauseMultiRegionClusterReplication [permission only]	Grants permission to pause replication for a Multi-Region cluster	Write	multiregioncluster*		
				aws:ResourceTag/${TagKey}	
PurchaseReservedNodesOffering	Grants permissions to purchase a new reserved node	Write	reservednode*		memorydb:TagResource
				aws:ResourceTag/${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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permissions to add up to 10 cost allocation tags to the named resource	Tagging	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			reservednode		
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource		Tagging	acl		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permissions to remove the tags identified by the TagKeys list from a resource		cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			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.

Note

The resource name in the ARN string should be lowercase to be effective.

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}

Resource types	ARN	Condition keys
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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	message could not be processed successfully, ensuring it cannot be replied to or delivered again				
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 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 AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateControlChannel	Grants permission to register a control channel for an instance to send control messages to Systems Manager service	Write		ssm:SourceInstanceARN 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	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	stream from an instance to Systems Manager service				

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 AWS 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 AWS 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 AWS Microservice Extractor for .NET

AWS Microservice Extractor for .NET (service prefix: `serviceextract`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Microservice Extractor for .NET

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConfig [permission only]	Grants permission to get required configuration for the AWS Microservice Extractor for .NET desktop client	Read			

Resource types defined by AWS Microservice Extractor for .NET

AWS Microservice Extractor for .NET does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Microservice Extractor for .NET, specify `"Resource": "*"` in your policy.

Condition keys for AWS Microservice Extractor for .NET

Microservice Extractor for .NET has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Migration Acceleration Program Credits

AWS Migration Acceleration Program Credits (service prefix: `mapcredits`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Migration Acceleration Program Credits
- Resource types defined by AWS Migration Acceleration Program Credits
- Condition keys for AWS Migration Acceleration Program Credits

Actions defined by AWS Migration Acceleration Program Credits

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssociatedPrograms [permission only]	Grants permission to view the user's associated Migration Acceleration Program agreements	List	agreement*		
ListQuarterCredits [permission only]	Grants permission to view Migration Acceleration Program agreements credits associated with the user's payer account	List	agreement*		
ListQuarterSpend [permission only]	Grants permission to view Migration Acceleration Program agreements eligible spend associated with the user's payer account	List	agreement*		

Resource types defined by AWS Migration Acceleration Program Credits

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
agreement	`arn:${Partition}:mapcredits:::${Agreement}/${AgreementId}`	

Condition keys for AWS Migration Acceleration Program Credits

MapCredits has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Migration Hub

AWS Migration Hub (service prefix: `mgh`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Migration Hub

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptConnection	Grants permission to accept a connection	Write	ConnectionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
AssociateAutomationUnitRole	Grants permission to associate an IAM role to an automation unit	Write	AutomationUnitResource*		
AssociateCreatedArtifact	Grants permission to associate a given AWS artifact to a MigrationTask	Write	migrationTask*		
AssociateDiscoveredResource	Grants permission to associate a given ADS resource to a MigrationTask	Write	migrationTask*		
AssociateSourceResource	Grants permission to associate source resource	Write	migrationTask*		
BatchAssociateIamRoleWithConnection	Grants permission to batch-associate IAM roles with a connection	Write	ConnectionResource*		
BatchDisassociateIamRoleFromConnection	Grants permission to batch-disassociate IAM roles from a connection	Write	ConnectionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutomationRun	Grants permission to create an automation unit run	Write			
CreateAutomationUnit	Grants permission to create an automation unit	Write			
CreateHomeRegionControl	Grants permission to create a Migration Hub Home Region Control	Write			
CreateProgressUpdateStream	Grants permission to create a ProgressUpdateStream	Write	progressUpdateStream*		
DeleteAutomationRun	Grants permission to delete an automation unit run	Write	AutomationRunResource*		
DeleteAutomationUnit	Grants permission to delete an automation unit	Write	AutomationUnitResource*		
DeleteConnection	Grants permission to delete a connection	Write	ConnectionResource*		
DeleteHomeRegionControl	Grants permission to delete a Migration Hub Home Region Control	Write			
DeleteProgressUpdateStream	Grants permission to delete a ProgressUpdateStream	Write	progressUpdateStream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeApplicationState	Grants permission to get an Application Discovery Service Application's state	Read			
DescribeAutomationRun	Grants permission to describe an automation unit run	Read	AutomationRunResource*		
DescribeAutomationUnit	Grants permission to describe an automation unit	Read	AutomationUnitResource*		
DescribeHomeRegionControls	Grants permission to list Home Region Controls	List			
DescribeMigrationTask	Grants permission to describe a MigrationTask	Read	migrationTask*		
DisassociateAutomationUnitRole	Grants permission to disassociate an IAM role from an automation unit	Write	AutomationUnitResource*		
DisassociateCreatedArtifact	Grants permission to disassociate a given AWS artifact from a MigrationTask	Write	migrationTask*		
DisassociateDiscoveredResource	Grants permission to disassociate a given ADS resource from a MigrationTask	Write	migrationTask*		
DisassociateSourceResource	Grants permission to diassociate source resource	Write	migrationTask*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConnection	Grants permission to get a connection	Read	ConnectionResource*		
GetHomeRegion	Grants permission to get the Migration Hub Home Region	Read			
ImportMigrationTask	Grants permission to import a MigrationTask	Write	migrationTask*		
ListApplicationStates	Grants permission to list Application statuses	List			
ListAutomationRuns	Grants permission to list automation unit runs	List			
ListAutomationUnits	Grants permission to list automation units	List			
ListConnectionRoles	Grants permission to list connection roles	List	ConnectionResource*		
ListConnections	Grants permission to list connections	List			
ListCreatedArtifacts	Grants permission to list associated created artifacts for a MigrationTask	List	migrationTask*		
ListDiscoveredResources	Grants permission to list associated ADS resources from MigrationTask	List	migrationTask*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMigrationTaskUpdates	Grants permission to list migration tasks updates	List	migrationTask*		
ListMigrationTasks	Grants permission to list MigrationTasks	List			
ListProgressUpdateStreams	Grants permission to to list ProgressUpdateStreams	List			
ListSourceResources	Grants permission to list source resources	List	migrationTask*		
ListTagsForResource	Grants permission to list tags for a resource	List			
NotifyApplicationState	Grants permission to update an Application Discovery Service Application's state	Write			
NotifyMigrationTaskState	Grants permission to notify latest MigrationTask state	Write	migrationTask*		
PutResourceAttributes	Grants permission to put ResourceAttributes	Write	migrationTask*		
RejectConnection	Grants permission to reject a connection	Write	ConnectionResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging		aws:TagKeys	

Resource types defined by AWS Migration 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
progressUpdateStream	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}`	
migrationTask	`arn:${Partition}:mgh:${Region}:${Account}:progressUpdateStream/${Stream}/migrationTask/${Task}`	
AutomationRunResource	`arn:${Partition}:mgh:${Region}:${Account}:automation-run/${RunID}`	mgh:AutomationRunResourceRunID

Resource types	ARN	Condition keys
AutomationUnitResource	arn:${Partition}:mgh:${Region}:${Account}:automation-unit/${AutomationUnitId}	mgh:AutomationUnitResourceAutomationUnitArn
ConnectionResource	arn:${Partition}:mgh:${Region}:${Account}:${ConnectionArn}	aws:ResourceTag/${TagKey} mgh:ConnectionResourceConnectionArn

Condition keys for AWS Migration Hub

AWS Migration Hub defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${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
mgh:AutomationRunResourceRunID	AutomationRunResource resource runID identifier	String

Condition keys	Description	Type
mgh:AutomationUnitResourceAutomationUnitArn	AutomationUnitResource resource automationUnitArn identifier	ARN
mgh:ConnectionResourceConnectionArn	ConnectionResource resource connectionArn identifier	String

Actions, resources, and condition keys for AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator (service prefix: `migrationhub-orchestrator`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Migration Hub Orchestrator
- Resource types defined by AWS Migration Hub Orchestrator
- Condition keys for AWS Migration Hub Orchestrator

Actions defined by AWS Migration Hub Orchestrator

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTemplate	Grants permission to create a custom template	Write			
CreateWorkflow	Grants permission to create a workflow based on the selected template	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkflowStep	Grants permission to create a step under a workflow and a specific step group	Write	workflow*		
CreateWorkflowStepGroup	Grants permission to to create a custom step group for a given workflow	Write	workflow*		
DeleteTemplate	Grants permission to delete a custom template	Write	template*		
DeleteWorkflow	Grants permission to a workflow	Write	workflow*		
DeleteWorkflowStep	Grants permission to delete a step from a specific step group under a workflow	Write	workflow*		
DeleteWorkflowStepGroup	Grants permission to delete a step group associated with a workflow	Write	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMessage	Grants permission to the plugin to receive information from the service	Read			
GetTemplate	Grants permission to get retrieve metadata for a Template	Read	template*		
GetTemplateStep	Grants permission to retrieve details of a step associated with a template and a step group	Read	template*		
GetTemplateStepGroup	Grants permission to retrieve metadata of a step group under a template	Read	template*		
GetWorkflow	Grants permission to retrieve metadata asscociated with a workflow	Read	workflow*		
GetWorkflowStep	Grants permission to get details of step associated with a workflow and a step group	Read	workflow*		
GetWorkflowStepGroup	Grants permission to get details of a step group associated with a workflow	Read	workflow*		
ListPlugins	Grants permission to get a list all registered Plugins	List			
ListTagsForResource		Read	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to get a list of all the tags tied to a resource		workflow*		
ListTemplateStepGroups	Grants permission to lists step groups of a template	List	template*		
ListTemplateSteps	Grants permission to get a list of steps in a step group	List	template*		
ListTemplates	Grants permission to get a list of all Templates available to customer	List			
ListWorkflowStepGroups	Grants permission to get list of step groups associated with a workflow	List	workflow*		
ListWorkflowSteps	Grants permission to get a list of steps within step group associated with a workflow	List	workflow*		
ListWorkflows	Grants permission to list all workflows	List			
RegisterPlugin	Grants permission to register the plugin to receive an ID and to start receiving messages from the service	Write			
RetryWorkflowStep	Grants permission to retry a failed step within a workflow	Write	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendMessage	Grants permission to the plugin to send information to the service	Write			
StartWorkflow	Grants permission to start a workflow or resume a stopped workflow	Write	workflow*		
StopWorkflow	Grants permission to stop a workflow	Write	workflow*		
TagResource	Grants permission to add tags to a resource	Tagging	template		
			workflow		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	template		
			workflow		
				aws:TagKeys	
UpdateTemplate	Grants permission to update a custom template	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWorkflow	Grants permission to update the metadata associated with the workflow	Write	workflow*		
UpdateWorkflowStep	Grants permission to update metadata and status of a custom step within a workflow	Write	workflow*		
UpdateWorkflowStepGroup	Grants permission to update metadata associated with a step group in a given workflow	Write	workflow*		

Resource types defined by AWS Migration Hub Orchestrator

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
workflow	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:workflow/${ResourceId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:migrationhub-orchestrator:${Region}:${Account}:template/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Migration Hub Orchestrator

AWS Migration Hub Orchestrator defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces (service prefix: `refactor-spaces`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Migration Hub Refactor Spaces

- Resource types defined by AWS Migration Hub Refactor Spaces
- Condition keys for AWS Migration Hub Refactor Spaces

Actions defined by AWS Migration Hub Refactor Spaces

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an application within an environment	Write		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Grants permission to create an environment	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRoute	Grants permission to create a route within an application	Write		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateService	Grants permission to create a service within an application	Write		refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Grants permission to delete an application from an environment	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
DeleteEnvironment	Grants permission to delete an environment	Write	environment*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Grants permission to delete a resource policy	Write			
DeleteRoute	Grants permission to delete a route from an application	Write	route*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteService	Grants permission to delete a service from an application	Write	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetApplication	Grants permission to get more information about an application	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
GetEnvironment	Grants permission to get more information for an environment	Read	environment*		
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Grants permission to get the details about a resource policy	Read			
GetRoute	Grants permission to get more information about a route	Read	route*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetService	Grants permission to get more information about a service	Read	service*		
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:CreatedByAccountIds aws:ResourceTag/${TagKey}	
ListApplications	Grants permission to list all the applications in an environment	Read	application*		
ListEnvironmentVpcs	Grants permission to list all the VPCs for the environment	Read	environment*		
ListEnvironments	Grants permission to list all environments	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRoutes	Grants permission to list all the routes in an application	Read	route*		
ListServices	Grants permission to list all the services in an environment	Read	environment*		
ListTagsForResource	Grants permission to list all the tags for a given resource	Read			
PutResourcePolicy	Grants permission to add a resource policy	Write			
TagResource	Grants permission to tag a resource	Tagging	application		
			environment		
			route		
			service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove a tag from a resource	Tagging	application		
			environment		
			route		
			service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:ResourceTag/${TagKey}	
UpdateRoute	Grants permission to update a route from an application	Write	route*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				refactor-spaces:ApplicationCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:RouteCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:SourcePath aws:ResourceTag/${TagKey}	

Resource types defined by AWS Migration Hub Refactor Spaces

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:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds
service	`arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/service/${ServiceId}`	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:ServiceCreatedByAccount

Resource types	ARN	Condition keys
route	arn:${Partition}:refactor-spaces:${Region}:${Account}:environment/${EnvironmentId}/application/${ApplicationId}/route/${RouteId}	aws:ResourceTag/${TagKey} refactor-spaces:ApplicationCreatedByAccount refactor-spaces:CreatedByAccountIds refactor-spaces:RouteCreatedByAccount refactor-spaces:ServiceCreatedByAccount refactor-spaces:SourcePath

Condition keys for AWS Migration Hub Refactor Spaces

AWS Migration Hub Refactor Spaces defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
refactor-spaces:ApplicationCreatedByAccount	Filters access by restricting the action to only those accounts that created the application within an environment	String
refactor-spaces:CreatedByAccountIds	Filters access by the accounts that created the resource	ArrayOfString
refactor-spaces:RouteCreatedByAccount	Filters access by restricting the action to only those accounts that created the route within an application	String
refactor-spaces:ServiceCreatedByAccount	Filters access by restricting the action to only those accounts that created the service within an application	String
refactor-spaces:SourcePath	Filters access by the path of the route	String

Actions, resources, and condition keys for AWS Migration Hub Strategy Recommendations

AWS Migration Hub Strategy Recommendations (service prefix: `migrationhub-strategy`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Migration Hub Strategy Recommendations

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAntiPattern	Grants permission to get details of each anti pattern that collector should look at in a customer's environment	Read			
GetApplicationComponentDetails	Grants permission to get details of an application	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApplicationComponentStrategies	Grants permission to get a list of all recommended strategies and tools for an application running in a server	Read			
GetAssessment	Grants permission to retrieve status of an on-going assessment	Read			
GetImportFileTask	Grants permission to get details of a specific import task	Read			
GetLatestAssessmentId	Grants permission to retrieve the latest assessment id	Read			
GetMessage	Grants permission to the collector to receive information from the service	Read			
GetPortfolioPreferences	Grants permission to retrieve customer migration/Modernization preferences	Read			
GetPortfolioSummary	Grants permission to retrieve overall summary (number-of servers to rehost etc as well as overall number of anti patterns)	Read			
GetRecommendationReportDetails	Grants permission to retrieve detailed information about a recommendation report	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServerDetails	Grants permission to get info about a specific server	Read			
GetServerStrategies	Grants permission to get recommended strategies and tools for a specific server	Read			
ListAnalyzableServers	Grants permission to get a list of all analyzable servers in a customer's vcenter environment	List			
ListAntiPatterns	Grants permission to get a list of all anti patterns that collector should look for in a customer's environment	List			
ListApplicationComponents	Grants permission to get a list of all applications running on servers on customer's servers	List			
ListCollectors	Grants permission to get a list of all collectors installed by the customer	List			
ListImportFileTask	Grants permission to get list of all imports performed by the customer	List			
ListJarArtifacts	Grants permission to get a list of binaries that collector should assess	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServers	Grants permission to get a list of all servers in a customer's environment	List			
PutLogData	Grants permission to the collector to send logs to the service	Write			
PutMetricData	Grants permission to the collector to send metrics to the service	Write			
PutPortfolioPreferences	Grants permission to save customer's Migration/ Modernization preferences	Write			
RegisterCollector	Grants permission to register the collector to receive an ID and to start receiving messages from the service	Write			
SendMessage	Grants permission to the collector to send information to the service	Write			
StartAssessment	Grants permission to start assessment in a customer's environment (collect data from all servers and provide recommendations)	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartImportFileTask	Grants permission to start importing data from a file provided by customer	Write			
StartRecommendationReportGeneration	Grants permission to start generating a recommendation report	Write			
StopAssessment	Grants permission to stop an on-going assessment	Write			
UpdateApplicationComponentConfig	Grants permission to update details for an application	Write			
UpdateCollectorConfiguration	Grants permission to the collector to send configuration information to the service	Write			
UpdateServerConfig	Grants permission to update info on a server along with the recommended strategy	Write			

Resource types defined by AWS Migration Hub Strategy Recommendations

AWS Migration Hub Strategy Recommendations does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Migration Hub Strategy Recommendations, specify `"Resource": "*"` in your policy.

Condition keys for AWS Migration Hub Strategy Recommendations

Migration Hub Strategy Recommendations has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Mobile Analytics

Amazon Mobile Analytics (service prefix: `mobileanalytics`) 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 Mobile Analytics
- Resource types defined by Amazon Mobile Analytics
- Condition keys for Amazon Mobile Analytics

Actions defined by Amazon Mobile 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFinancialReports	Grant access to financial metrics for an app	Read			
GetReports	Grant access to standard metrics for an app	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEvents	The PutEvents operation records one or more events	Write			

Resource types defined by Amazon Mobile Analytics

Amazon Mobile Analytics does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Mobile Analytics, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Mobile Analytics

Mobile Analytics has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Monitron

Amazon Monitron (service prefix: `monitron`) 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 Monitron
- Resource types defined by Amazon Monitron
- Condition keys for Amazon Monitron

Actions defined by Amazon Monitron

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateProjectAdminUser [permission only]	Grants permission to associate a user with the project as an administrator	Permissions management	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProject [permission only]	Grants permission to create a project	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole kms:CreateGrant sso:CreateManagedApplicationInstance sso:DeleteManagedApplicationInstance sso:DescribeRegisteredRegions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProjectUserAssociation [permission only]	Grants permission to associate a user with the project	Permissions management	project*		sso-directory:DescribeUsers sso:AssociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUserAccessRoleAssociation [permission only]	Grants permission to associate an access role with the user	Permissions management	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
DeleteProject [permission only]	Grants permission to delete a project	Write	project*		sso:DeleteManagedApplicationInstance

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProjectUserAssociation [permission only]	Grants permission to disassociate a user from the project	Permissions management	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
DeleteUserAccessRoleAssociation [permission only]	Grants permission to disassociate an access role from the user	Permissions management	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateProjectAdminUser [permission only]	Grants permission to disassociate an administrator from the project	Permissions management	project*		sso-directory:DescribeUsers sso:DisassociateProfile sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfiles
GetProject [permission only]	Grants permission to get information about a project	Read	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProjectAdminUser [permission only]	Grants permission to describe an administrator who is associated with the project	Read	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance sso:ListProfileAssociations
ListProjectAdminUsers [permission only]	Grants permission to list all administrators associated with the project	Permissions management	project*		sso-directory:DescribeUsers sso:GetManagedApplicationInstance

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProjectUserAssociations [permission only]	Grants permission to list all users associated with the project	List	project*		sso:GetManagedApplicationInstance sso:GetProfile sso:ListDirectoryAssociations sso:ListProfileAssociations sso:ListProfiles
ListProjects [permission only]	Grants permission to list all projects	List			
ListTagsForResource [permission only]	Grants permission to list all tags for a resource	Read	project		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListUserAccessRoleAssociations [permission only]	Grants permission to list all access roles associated with the user	List	project*		
TagResource [permission only]	Grants permission to tag a resource	Tagging	project		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [permission only]	Grants permission to untag a resource	Tagging	project		
				aws:TagKeys	
UpdateProject [permission only]	Grants permission to update a project	Write	project*		

Resource types defined by Amazon Monitron

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:${Partition}:monitron:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Monitron

Amazon Monitron defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBroker	Grants permission to create a broker	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateVpcEndpoint ec2:DescribeIntern

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					etGateways ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole route53:AssociateVPCWithHostedZone
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser	Grants permission to create an ActiveMQ user	Write	brokers*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBroker	Grants permission to return information about the specified broker	Read	brokers*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTags	Grants permission to return a list of tags	List	brokers		
			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*		
UpdateBrokerAccessConfiguration [permission only]	Grants permission to update RabbitMQ broker authentication and authorization configuration	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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Multi-party approval

Multi-party approval (service prefix: `mpa`) 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 Multi-party approval
- Resource types defined by Multi-party approval
- Condition keys for Multi-party approval

Actions defined by Multi-party approval

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelSession	Grants permission to cancel an approval session	Write	session*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
CreateApprovalTeam	Grants permission to create an approval team	Write	approval-team*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateIdentitySource	Grants permission to create an identity source	Write	identity-source*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteIdentitySource	Grants permission to delete an identity source	Write	identity-source*		
				aws:ResourceTag/${TagKey}	
DeleteInactiveApprovalTeamVersion	Grants permission to delete an inactive approval team	Write	approval-team*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [permission only]	Grants permission to delete a resource policy	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApprovalTeam	Grants permission to retrieve details for an approval team	Read	approval-team*		
				aws:ResourceTag/${TagKey}	
GetIdentitySource	Grants permission to retrieve details for an identity source	Read	identity-source*		
				aws:ResourceTag/${TagKey}	
GetPolicyVersion	Grants permission to retrieve details for a policy	Read			
GetResourcePolicy	Grants permission to retrieve details for a specific resource	Read			
GetSession	Grants permission to retrieve details for an approval session	Read	session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
ListApprovalTeams	Grants permission to list approval teams	List			
ListIdentitySources	Grants permission to list identity sources	List			
ListPolicies	Grants permission to list policies	List			
ListPolicyVersions	Grants permission to list the versions for policies	List			
ListResourcePolicies	Grants permission to list policies for a resource	List			
ListSessions	Grants permission to list approval sessions	List			
ListTagsForResource	Grants permission to list tags for a resource	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy [permission only]	Grants permission to create or update policies for a resource	Permissions management			
StartActiveApprovalTeamDeletion	Grants permission to start the deletion process for an active approval team	Write	approval-team*		
				aws:ResourceTag/${TagKey}	
StartApprovalTeamBaseline	Grants permission to start a baseline for an active approval team	Write	approval-team*		
				aws:ResourceTag/${TagKey}	
StartSession [permission only]	Grants permission to start an approval session	Write	session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} mpa:RequestedOperation mpa:ProtectedResourceAccount	
TagResource	Grants permission to tag a resource	Tagging		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag a resource	Tagging		aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateApprovalTeam	Grants permission to update approval team	Write	approval-team*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Multi-party approval

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
approval-team	`arn:${Partition}:mpa:${Region}:${Account}:approval-team/${ApprovalTeamId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
identity-source	arn:${Partition}:mpa:${Region}:${Account}:identity-source/${IdentitySourceId}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:mpa:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}

Condition keys for Multi-party approval

Multi-party approval defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
mpa:ProtectedResourceAccount	Filters access by the account that owns the resource that is the target of the operation that requires approval	String
mpa:RequestedOperation	Filters access by a requested operation that requires team approval before it can be executed	String

Actions, resources, and condition keys for AWS MWAA Serverless

AWS MWAA Serverless (service prefix: `airflow-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 AWS MWAA 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflow	Grants permission to create a new workflow	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteWorkflow	Grants permission to delete a workflow	Write	Workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTaskInstance	Grants permission to retrieve the task details for a workflow run	Read	Workflow*		
GetWorkflow	Grants permission to retrieve details about a workflow	Read	Workflow*		
GetWorkflowRun	Grants permission to retrieve details about a workflow run	Read	Workflow*		
ListTagsForResource	Grants permission to list the tags for the specified resource	Read	Workflow*		
				aws:ResourceTag/${TagKey}	
ListTaskInstances	Grants permission to list the tasks for a workflow run	List	Workflow*		
ListWorkflowRuns	Grants permission to list the workflow runs of a workflow	List	Workflow*		
ListWorkflowVersions	Grants permission to list the workflow versions	List	Workflow*		
ListWorkflows	Grants permission to list the workflows	List			
StartWorkflowRun	Grants permission to start an on-demand workflow run for the workflow	Write	Workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopWorkflowRun	Grants permission to stop a workflow run	Write	Workflow*		
TagResource	Grants permission to tag the specified resource	Tagging	Workflow*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag the specified resource	Tagging	Workflow*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateWorkflow	Grants permission to update an existing workflow	Write	Workflow*		

Resource types defined by AWS MWAA 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
Workflow	`arn:${Partition}:airflow-serverless:${Region}:${Account}:workflow/${WorkflowId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS MWAA Serverless

AWS MWAA 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs that are attached to the resource	String
aws:TagKeys	Filters access by tag keys 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelMLModelTransformJob	Grants permission to cancel an ML model transform job	Write	database*		
CancelQuery	Grants permission to cancel a query	Write	database*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLoaderJobs	Grants permission to list all the loader jobs	List	database*		
ListMLDataProcessingJobs	Grants permission to list all the ML data processing jobs	List	database*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMLDataProcessingJob	Grants permission to start an ML data processing job	Write	database*		
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 AWS global condition context keys.

Condition keys	Description	Type
neptune-db:QueryLanguage	Filters access by graph model	String

Actions, resources, and condition keys for Amazon Neptune Analytics

Amazon Neptune Analytics (service prefix: `neptune-graph`) 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 Analytics
- Resource types defined by Amazon Neptune Analytics

- Condition keys for Amazon Neptune Analytics

Actions defined by Amazon Neptune 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

All IAM actions except 'ReadDataViaQuery', 'WriteDataViaQuery' and 'DeleteDataViaQuery' have a corresponding API operation

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelExportTask	Grants permission to cancel an ongoing export task	Write	export-task*		
				aws:ResourceTag/${TagKey}	
CancelImportTask	Grants permission to cancel an ongoing import task	Write	import-task*		
CancelQuery	Grants permission to cancel a query	Write	graph*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGraph	Grants permission to create a new graph	Write	graph*		iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
CreateGraphSnapshot	Grants permission to create a new snapshot from an existing graph	Write	graph*		
			graph-snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateGraphUsingImportTask	Grants permission to create a new graph while importing data into the new graph	Write	graph*		iam:CreateServiceLinkedRole iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey
			import-task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePrivateGraphEndpoint	Grants permission to create a new private graph endpoint to access the graph from within a vpc	Write	graph*		ec2:CreateVpcEndpoint ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:AssociateV

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					PCWithHostedZone
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteDataViaQuery	Grants permission to delete data via query APIs on the graph	Write	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraph	Grants permission to delete a graph	Write	graph*		
				aws:ResourceTag/${TagKey}	
DeleteGraphSnapshot	Grants permission to delete a snapshot	Write	graph-snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePrivateGraphEndpoint	Grants permission to delete a private graph endpoint of a graph	Write	graph*		ec2:DeleteVpcEndpoints ec2:DescribeAvailabilityZones ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyVpcEndpoint route53:Disassocia

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					teVPCFromHostedZone
				aws:ResourceTag/${TagKey}	
GetEngineStatus	Grants permission to get the engine status of the graph	Read	graph*		
				aws:ResourceTag/${TagKey}	
GetExportTask	Grants permission to get details about an export task	Read	export-task*		
				aws:ResourceTag/${TagKey}	
GetGraph	Grants permission to get details about a graph	Read	graph*		
				aws:ResourceTag/${TagKey}	
GetGraphSnapshot	Grants permission to get details about a snapshot	Read	graph-snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetGraphSummary	Grants permission to get the summary for the data in the graph	Read	graph*		
				aws:ResourceTag/${TagKey}	
GetImportTask	Grants permission to get details about an import task	Read	import-task*		
GetPrivateGraphEndpoint	Grants permission to get details about a private graph endpoint of a graph	Read	graph*		
				aws:ResourceTag/${TagKey}	
GetQueryStatus	Grants permission to check the status of a given query	Read	graph*		
				aws:ResourceTag/${TagKey}	
GetStatisticsStatus	Grants permission to get the statistics for the data in the graph	Read	graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListExportTasks	Grants permission to list the export tasks in your account	Read	export-task*		
ListGraphSnapshots	Grants permission to list the snapshots in your account	Read	graph-snapshot*		
ListGraphs	Grants permission to list the graphs in your account	Read	graph*		
ListImportTasks	Grants permission to list the import tasks in your account	Read	import-task*		
ListPrivateGraphEndpoints	Grants permission to list the private graph endpoints for a given graph	Read	graph*		
				aws:ResourceTag/${TagKey}	
ListQueries	Grants permission to check the status of all active queries	Read	graph*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource		Read	graph		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to lists tag for a Neptune Analytics resource		graph-snapshot		
				aws:ResourceTag/${TagKey}	
ReadDataViaQuery	Grants permission to read data via query APIs on the graph	Read	graph*		
				aws:ResourceTag/${TagKey}	
ResetGraph	Grants permission to reset a graph which deletes all data within the graph	Write	graph*		
				aws:ResourceTag/${TagKey}	
RestoreGraphFromSnapshot	Grants permission to create a new graph from an existing snapshot	Write	graph*		kms:CreateGrant kms:Decrypt kms:DescribeKey
			graph-snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys neptune-graph:PublicConnectivity	
StartExportTask	Grants permission to export data from an existing graph	Write	export-task* graph*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StartGraph	Grants permission to start a graph	Write	graph*		kms:Decrypt kms:DescribeKey
				aws:ResourceTag/${TagKey}	
StartImportTask	Grants permission to import data into an existing graph	Write	graph*		iam:PassRole
			import-task*		
StopGraph	Grants permission to stop a graph	Write	graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a Neptune Analytics resource	Tagging	graph		
			graph-snapshot		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a Neptune Analytics resource	Tagging	graph		
			graph-snapshot		
				aws:TagKeys	
UpdateGraph	Grants permission to modify a graph	Write	graph*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} neptune-graph:PublicConnectivity	
WriteDataViaQuery	Grants permission to write data via query APIs on the graph	Write	graph*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Neptune 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
graph	`arn:${Partition}:neptune-graph:${Region}:${Account}:graph/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
graph-snapshot	arn:${Partition}:neptune-graph:${Region}:${Account}:graph-snapshot/${ResourceId}	aws:ResourceTag/${TagKey}
import-task	arn:${Partition}:neptune-graph:${Region}:${Account}:import-task/${ResourceId}	
export-task	arn:${Partition}:neptune-graph:${Region}:${Account}:export-task/${ResourceId}	

Condition keys for Amazon Neptune Analytics

Amazon Neptune 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 AWS 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

Condition keys	Description	Type
neptune-graph:PublicConnectivity	Filters access by the value of the public connectivity parameter provided in the request or its default value, if unspecified. All access to graphs is IAM authenticated	Bool

Actions, resources, and condition keys for AWS Network Firewall

AWS 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 AWS Network Firewall
- Resource types defined by AWS Network Firewall
- Condition keys for AWS Network Firewall

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptNetworkFirew	Grants permission to accept pending Network Firewall	Write	Firewall*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
allTransitGatewayAttachment	attachments on a transit gateway				
AssociateAvailabilityZones	Grants permission to associate availability zones to a firewall	Write	Firewall*		
AssociateFirewallPolicy	Grants permission to create an association between a firewall policy and a firewall	Write	Firewall*		
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateSubnets	Grants permission to associate VPC subnets to a firewall	Write	Firewall*		
AttachRuleGroupsToProxyConfiguration	Grants permission to attach proxy rule groups to a proxy configuration	Write	ProxyConfiguration*		
			ProxyRuleGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFirewall	Grants permission to create an AWS Network Firewall firewall	Write	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	Grants permission to create an AWS Network Firewall firewall policy	Write	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxy	Grants permission to create an AWS Network Firewall proxy	Write	Proxy*		ec2:AttachApplianceToNatGateway
			ProxyConfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxyConfiguration	Grants permission to create an AWS Network Firewall proxy configuration	Write	ProxyConfiguration*		
			ProxyRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxyRuleGroup	Grants permission to create an AWS Network Firewall proxy rule group	Write	ProxyRuleGroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProxyRules	Grants permission to add proxy rules to a proxy rule group	Write	ProxyRuleGroup*		
CreateRuleGroup	Grants permission to create an AWS Network Firewall rule group	Write	StatefulRuleGroup		
			StatelessRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	Grants permission to create an AWS Network Firewall tls inspection configuration	Write	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcEndpointAssociation	Grants permission to create an AWS Network Firewall vpc endpoint association	Write	Firewall*		iam:CreateServiceLinkedRole
			VpcEndpointAssociation*		

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*		
DeleteNetworkFirewallTransitGatewayAttachment	Grants permission to delete Network Firewall attachments on a transit gateway	Write	Firewall*		
DeleteProxy	Grants permission to delete a proxy	Write	Proxy*		ec2:DetachApplianceFromNatGateway
DeleteProxyConfiguration	Grants permission to delete a proxy configuration	Write	ProxyConfiguration*		
DeleteProxyRuleGroup	Grants permission to delete a proxy rule group	Write	ProxyRuleGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProxyRules	Grants permission to remove proxy rules from a proxy rule group	Write	ProxyRuleGroup*		
DeleteResourcePolicy	Grants permission to delete a resource policy for a firewall policy or rule group or firewall	Write	Firewall		
			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*		
DeleteVpcEndpointAssociation	Grants permission to delete a vpc endpoint association	Write	VpcEndpointAssociation*		
DescribeFirewall	Grants permission to retrieve the data objects that define a firewall	Read	Firewall*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFirewallMetadata	Grants permission to retrieve the high-level information about 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
DescribeProxy	Grants permission to retrieve the data objects that define a proxy	Read	Proxy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProxyConfiguration	Grants permission to retrieve the data objects that define a proxy configuration	Read	ProxyConfiguration*		
DescribeProxyRule	Grants permission to retrieve the data objects that define a proxy rule	Read	ProxyRuleGroup*		
DescribeProxyRuleGroup	Grants permission to retrieve the data objects that define a proxy rule group	Read	ProxyRuleGroup*		
DescribeResourcePolicy	Grants permission to describe a resource policy for a firewall policy or rule group or firewall	Read	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRuleGroupSummary	Grants permission to retrieve the summary information about a rule group	Read	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	Grants permission to retrieve the data objects that define a tls inspection configuration	Read	TLSInspectionConfiguration*		
DescribeVpcEndpointAssociation	Grants permission to retrieve the data objects that define a vpc endpoint association	Read	VpcEndpointAssociation*		
DetachRuleGroupsFromProxyConfiguration	Grants permission to detach proxy rule groups from a proxy configuration	Write	ProxyConfiguration*		
			ProxyRuleGroup*		
DisassociateAvailabilityZones	Grants permission to disassociate availability zones to a firewall	Write	Firewall*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAnalysisReports	Grants permission to list firewall analysis reports	List	Firewall*		
ListFirewallPolicies	Grants permission to retrieve the metadata for firewall policies	List	FirewallPolicy*		
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*		
ListProxies	Grants permission to retrieve the metadata for proxies	List	Proxy*		
ListProxyConfigurations	Grants permission to retrieve the metadata for proxy configurations	List	ProxyConfiguration*		
ListProxyRuleGroups	Grants permission to retrieve the metadata for proxy rule groups	List	ProxyRuleGroup*		
ListRuleGroups	Grants permission to retrieve the metadata for rule groups	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			VpcEndpointAssociation		
ListVpcEndpointAssociations	Grants permission to retrieve the metadata for vpc endpoint associations	List	VpcEndpointAssociation*		
PutResourcePolicy	Grants permission to put a resource policy for a firewall policy or rule group or firewall	Write	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Stateless RuleGroup		
RejectNetworkFirewallTransitGatewayAttachment	Grants permission to reject pending Network Firewall attachments on a transit gateway	Write	Firewall*		
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		
			Proxy		
			ProxyConfiguration		
			ProxyRuleGroup		
			StatefulRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Stateless RuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	Firewall		
			FirewallPolicy		
			Proxy		
			ProxyConfiguration		
			ProxyRuleGroup		
			StatefulRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Stateless RuleGroup		
			TLSInspectionConfiguration		
			VpcEndpointAssociation		
				aws:TagKeys	
UpdateAvailabilityZoneChangeProtection	Grants permission to add or remove availability zone change protection for a firewall	Write	Firewall*		
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*		
UpdateFirewallDescription	Grants permission to modify the description for a firewall	Write	Firewall*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateProxy	Grants permission to modify a proxy	Write	Proxy*		
UpdateProxyConfiguration	Grants permission to modify a proxy configuration	Write	ProxyConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProxyRule	Grants permission to update an existing proxy rule on a proxy rule group	Write	ProxyRuleGroup*		
UpdateProxyRuleGroupPriorities	Grants permission to modify rule group priorities on a proxy configuration	Write	ProxyConfiguration*		
UpdateProxyRulePriorities	Grants permission to update proxy rule priorities within a proxy rule group	Write	ProxyRuleGroup*		
UpdateRuleGroup	Grants permission to modify a rule group	Write	StatefulRuleGroup		
			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 AWS 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}
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/${TagKey}
VpcEndpointAssociation	arn:${Partition}:network-firewall:${Region}:${Account}:vpc-endpoint-association/${Name}	aws:ResourceTag/${TagKey}
ProxyRuleGroup	arn:${Partition}:network-firewall:${Region}:${Account}:proxy-rule-group/${Name}	aws:ResourceTag/${TagKey}
ProxyConfiguration	arn:${Partition}:network-firewall:${Region}:${Account}:proxy-configuration/${Name}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Proxy	`arn:${Partition}:network-firewall:${Region}:${Account}:proxy/${Name}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Network Firewall

AWS 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 AWS 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 Network Flow Monitor

Network Flow Monitor (service prefix: `networkflowmonitor`) 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 Network Flow Monitor

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMonitor	Grants permission to create a monitor	Write	monitor*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScope	Grants permission to create a scope	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMonitor	Grants permission to delete a monitor	Write	monitor*		
DeleteScope	Grants permission to delete a scope	Write	scope*		
GetMonitor	Grants permission to get information about a monitor	Read	monitor*		
GetQueryResultsMonitorTopContributors	Grants permission to get the results of a query that retrieves top contributors data for a monitor	Read	monitor*		
GetQueryResultsWorkloadInsightsTopContributors	Grants permission to get the results of a query that retrieves top contributors for workload insights	Read	scope*		
GetQueryResultsWorkloadInsightsTopContributorsData	Grants permission to get the results of a query that retrieves top contributors data points for workload insights	Read	scope*		
GetQueryStatusMonitorTopContributors	Grants permission to get the status of a query that retrieves top contributors data for a monitor	Read	monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQueryStatusWorkloadInsightsTopContributors	Grants permission to get the status of a query that retrieves top contributors for workload insights	Read	scope*		
GetQueryStatusWorkloadInsightsTopContributorsData	Grants permission to get the status of a query that retrieves top contributors data points for workload insights	Read	scope*		
GetScope	Grants permission to get information about a scope	Read	scope*		
ListMonitors	Grants permission to list all monitors in an account and their statuses	List			
ListScopes	Grants permission to get all scopes for an account	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	monitor scope		
Publish	Grants permission to publish a report	Write			
StartQueryMonitorTopContributors	Grants permission to start a query for retrieving top contributors data for a monitor	Write	monitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartQueryWorkloadInsightsTopContributors	Grants permission to start a query for retrieving top contributors data for workload insights	Write	scope*		
StartQueryWorkloadInsightsTopContributorsData	Grants permission to start a query for retrieving top contributors data points for workload insights	Write	scope*		
StopQueryMonitorTopContributors	Grants permission to stop a query for retrieving top contributors data for a monitor	Write	monitor*		
StopQueryWorkloadInsightsTopContributors	Grants permission to stop a query for retrieving top contributors for workload insights	Write	scope*		
StopQueryWorkloadInsightsTopContributorsData	Grants permission to stop a query for retrieving top contributors data points for workload insights	Write	scope*		
TagResource	Grants permission to add tags to a resource	Tagging	monitor scope		

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	monitor		
			scope		
				aws:TagKeys	
UpdateMonitor	Grants permission to update a monitor	Write	monitor*		
UpdateScope	Grants permission to update a scope	Write	scope*		

Resource types defined by Network Flow Monitor

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
monitor	arn:${Partition}:networkflowmonitor:${Region}:${Account}:monitor/${MonitorName}	aws:ResourceTag/${TagKey}
scope	arn:${Partition}:networkflowmonitor:${Region}:${Account}:scope/${ScopeId}	aws:ResourceTag/${TagKey}

Condition keys for Network Flow Monitor

Network Flow Monitor defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Network Manager

AWS Network Manager (service prefix: networkmanager) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Network Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAttachment	Grants permission to accept creation of an attachment between a source and destination in a core network	Write	attachment*		ec2:DescribeRegions
AssociateConnectPeer	Grants permission to associate a Connect Peer	Write	device*		
			global-network*		
AssociateCustomerGateway	Grants permission to associate a customer gateway to a device	Write	device*		
			global-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			link		
				networkmanager:cgwArn	
Associate Link	Grants permission to associate a link to a device	Write	device*		
			global-network*		
			link*		
Associate TransitGatewayConnectPeer	Grants permission to associate a transit gateway connect peer to a device	Write	device*		
			global-network*		
			link		
				networkmanager:tgwConnectPeerArn	
CreateConnectAttachment	Grants permission to create a Connect attachment	Write	attachment*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			core-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectPeer	Grants permission to create a Connect Peer connection	Write	attachment*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnection	Grants permission to create a new connection	Write	global-network*		networkmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetwork	Grants permission to create a new core network	Write	global-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCoreNetworkPrefixListAssociation	Grants permission to create a prefix list core network association	Write	core-network*		
CreateDevice	Grants permission to create a new device	Write	global-network*		networkmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGatewayAttachment	Grants permission to create a Direct Connect gateway attachment	Write	core-network*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:directConnectGatewayArn networkmanager:edgeLocations	
CreateGlobalNetwork	Grants permission to create a new global network	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole networkmanager:TagResource
CreateLink	Grants permission to create a new link	Write	global-network*		networkmanager:TagResource
			site		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSite	Grants permission to create a new site	Write	global-network*		networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSiteToSiteVpnAttachment	Grants permission to create a site-to-site VPN attachment	Write	core-network*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpnConnectionArn	
CreateTransitGatewayPeering	Grants permission to create a Transit Gateway peering	Write	core-network*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayRouteTableAttachment	Grants permission to create a TGW RTB attachment	Write	peering*		ec2:DescribeRegions networkmanager:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:tgwRtbArn	
CreateVpcAttachment	Grants permission to create a VPC attachment	Write	core-network*		ec2:DescribeRegions networkmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:vpcArn networkmanager:subnetArns	
DeleteAttachment	Grants permission to delete an attachment	Write	attachment*		ec2:DescribeRegions
DeleteConnectPeer	Grants permission to delete a Connect Peer	Write	connect-peer*		ec2:DescribeRegions
DeleteConnection	Grants permission to delete a connection	Write	connection*		
			global-network*		
DeleteCoreNetwork	Grants permission to delete a core network	Write	core-network*		ec2:DescribeRegions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCoreNetworkPolicyVersion	Grants permission to delete the core network policy version	Write	core-network*		
DeleteCoreNetworkPrefixListAssociation	Grants permission to delete a prefix list core network association	Write	core-network*		
DeleteDevice	Grants permission to delete a device	Write	device*		
			global-network*		
DeleteGlobalNetwork	Grants permission to delete a global network	Write	global-network*		
DeleteLink	Grants permission to delete a link	Write	global-network*		
			link*		
DeletePeering	Grants permission to delete a peering	Write	peering*		ec2:DescribeRegions
DeleteResourcePolicy	Grants permission to delete a resource	Permissions management	core-network*		
DeleteSite	Grants permission to delete a site	Write	global-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			site*		
DeregisterTransitGateway	Grants permission to deregister a transit gateway from a global network	Write	global-network*		
				networkmanager:tgwArn	
DescribeGlobalNetworks	Grants permission to describe global networks	List	global-network		
DisassociateConnectPeer	Grants permission to disassociate a Connect Peer	Write	global-network*		
DisassociateCustomerGateway	Grants permission to disassociate a customer gateway from a device	Write	global-network*		
				networkmanager:cgwArn	
DisassociateLink	Grants permission to disassociate a link from a device	Write	device*		
			global-network*		
			link*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayConnectPeer	Grants permission to disassociate a transit gateway connect peer from a device	Write	global-network*		
				networkmanager:tgwConnectPeerArn	
ExecuteCoreNetworkChangeSet	Grants permission to apply changes to the core network	Write	core-network*		ec2:DescribeRegions
GetConnectAttachment	Grants permission to retrieve a Connect attachment	Read	attachment*		
GetConnectPeer	Grants permission to retrieve a Connect Peer	Read	connect-peer*		
GetConnectPeerAssociations	Grants permission to describe Connect Peer associations	Read	global-network*		
GetConnections	Grants permission to describe connections	List	global-network*		
			connection		
GetCoreNetwork	Grants permission to retrieve a core network	Read	core-network*		
GetCoreNetworkChangeEvents	Grants permission to retrieve a list of core network change events	Read	core-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCoreNetworkChangeSet	Grants permission to retrieve a list of core network change sets	Read	core-network*		
GetCoreNetworkPolicy	Grants permission to retrieve core network policy	Read	core-network*		
GetCustomerGatewayAssociations	Grants permission to describe customer gateway associations	List	global-network*		
GetDevices	Grants permission to describe devices	List	global-network*		
			device		
GetDirectConnectGatewayAttachment	Grants permission to retrieve a Direct Connect gateway attachment	Read	attachment*		
GetLinkAssociations	Grants permission to describe link associations	List	global-network*		
			device		
			link		
GetLinks	Grants permission to describe links	List	global-network*		
			link		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetworkResourceCounts	Grants permission to return the number of resources for a global network grouped by type	Read	global-network*		
GetNetworkResourceRelationships	Grants permission to retrieve related resources for a resource within the global network	Read	global-network*		
GetNetworkResources	Grants permission to retrieve a global network resource	Read	global-network*		
GetNetworkRoutes	Grants permission to retrieve routes for a route table within the global network	Read	global-network*		
GetNetworkTelemetry	Grants permission to retrieve network telemetry objects for the global network	Read	global-network*		
GetResourcePolicy	Grants permission to retrieve a resource policy	Read	core-network*		
GetRouteAnalysis	Grants permission to retrieve a route analysis configuration and result	Read	global-network*		
GetSiteToSiteVpnAttachment	Grants permission to retrieve a site-to-site VPN attachment	Read	attachment*		
GetSites	Grants permission to describe global networks	List	global-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			site		
GetTransitGatewayConnectPeerAssociations	Grants permission to describe transit gateway connect peer associations	List	global-network*		
GetTransitGatewayPeering	Grants permission to retrieve a Transit Gateway peering	Read	peering*		
GetTransitGatewayRegistrations	Grants permission to describe transit gateway registrations	List	global-network*		
GetTransitGatewayRouteTableAttachment	Grants permission to retrieve a TGW RTB attachment	Read	attachment*		
GetVpcAttachment	Grants permission to retrieve a VPC attachment	Read	attachment*		
ListAttachmentRoutingPolicyAssociations	Grants permission to list all routing policies associated to core network attachments	List	core-network*		
ListAttachments	Grants permission to describe attachments	List	attachment*		
ListConnectPeers	Grants permission to describe Connect Peers	List	connect-peer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCoreNetworkPolicyVersions	Grants permission to list core network policy versions	List	core-network*		
ListCoreNetworkPrefixListAssociations	Grants permission to list core network prefix list associaitons	List	core-network*		
ListCoreNetworkRoutingInformation	Grants permission to list core network routing information	List	core-network*		
ListCoreNetworks	Grants permission to list core networks	List			
ListOrganizationServiceAccessStatus	Grants permission to list organization service access status	List			
ListPeerings	Grants permission to describe peerings	List			
ListTagsForResource	Grants permission to list tags for a Network Manager resource	Read	attachment		
			connect-peer		
			connection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:ResourceTag/${TagKey}	
PutAttachmentRoutingPolicyLabel	Grants permission to put an attachment routing policy label	Write	attachment*		
			core-network*		
PutCoreNetworkPolicy	Grants permission to create a core network policy	Write	core-network*		ec2:DescribeRegions
PutResourcePolicy	Grants permission to create or update a resource policy	Permissions management	core-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterTransitGateway	Grants permission to register a transit gateway to a global network	Write	global-network*		
				networkmanager:tgwArn	
RejectAttachment	Grants permission to reject attachment request	Write	attachment*		
RemoveAttachmentRoutingPolicyLabel	Grants permission to remove an attachment routing policy label	Write	attachment*		
			core-network*		
RestoreCoreNetworkPolicyVersion	Grants permission to restore the core network policy to a previous version	Write	core-network*		ec2:DescribeRegions
StartOrganizationServiceAccessUpdate	Grants permission to start organization service access update	Permissions management			
StartRouteAnalysis	Grants permission to start a route analysis and stores analysis configuration	Write	global-network*		
TagResource	Grants permission to tag a Network Manager resource	Tagging	attachment		
			connect-peer		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a Network Manager resource	Tagging	attachment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			connect-peer		
			connection		
			core-network		
			device		
			global-network		
			link		
			peering		
			site		
				aws:TagKeys	
UpdateConnection	Grants permission to update a connection	Write	connection*		
			global-network*		
UpdateCoreNetwork	Grants permission to update a core network	Write	core-network*		
UpdateDevice	Grants permission to update a device	Write	device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			global-network*		
UpdateDirectConnectGatewayAttachment	Grants permission to update a Direct Connect gateway attachment	Write	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:edgeLocations	
UpdateGlobalNetwork	Grants permission to update a global network	Write	global-network*		
UpdateLink	Grants permission to update a link	Write	global-network*		
			link*		
UpdateNetworkResourceMetadata	Grants permission to add or update metadata key/value pairs on network resource	Write	global-network*		
UpdateSite	Grants permission to update a site	Write	global-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			site*		
UpdateVpcAttachment	Grants permission to update a VPC attachment	Write	attachment*		ec2:DescribeRegions
				aws:RequestTag/${TagKey} aws:TagKeys networkmanager:subnetArns	

Resource types defined by AWS Network 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
global-network	`arn:${Partition}:networkmanager::${Account}:global-network/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
site	arn:${Partition}:networkmanager::${Account}:site/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
link	arn:${Partition}:networkmanager::${Account}:link/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
device	arn:${Partition}:networkmanager::${Account}:device/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
connection	arn:${Partition}:networkmanager::${Account}:connection/${GlobalNetworkId}/${ResourceId}	aws:ResourceTag/${TagKey}
core-network	arn:${Partition}:networkmanager::${Account}:core-network/${ResourceId}	aws:ResourceTag/${TagKey}
attachment	arn:${Partition}:networkmanager::${Account}:attachment/${ResourceId}	aws:ResourceTag/${TagKey}
connect-peer	arn:${Partition}:networkmanager::${Account}:connect-peer/${ResourceId}	aws:ResourceTag/${TagKey}
peering	arn:${Partition}:networkmanager::${Account}:peering/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Network Manager

AWS Network Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
networkmanager:cgwArn	Filters access by which customer gateways can be associated or disassociated	ARN
networkmanager:directConnectGatewayArn	Filters access by which Direct Connect gateway can be used to a create/update attachment	ARN
networkmanager:edgeLocations	Filters access by which edge locations can be added or removed from a Direct Connect gateway attachment	ArrayOfString
networkmanager:subnetArns	Filters access by which VPC subnets can be added or removed from a VPC attachment	ArrayOfARN
networkmanager:tgwArn	Filters access by which transit gateways can be registered, deregistered, or peered	ARN
networkmanager:tgwConnectPeerArn	Filters access by which transit gateway connect peers can be associated or disassociated	ARN

Condition keys	Description	Type
networkmanager:tgwRtbArn	Filters access by which Transit Gateway Route Table can be used to create an attachment	ARN
networkmanager:vpcArn	Filters access by which VPC can be used to a create/update attachment	ARN
networkmanager:vpnConnectionArn	Filters access by which Site-to-Site VPN can be used to a create/update attachment	ARN

Actions, resources, and condition keys for AWS Network Manager Chat

AWS Network Manager Chat (service prefix: `networkmanager-chat`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Network Manager Chat
- Resource types defined by AWS Network Manager Chat
- Condition keys for AWS Network Manager Chat

Actions defined by AWS Network Manager Chat

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelMessageResponse [permission only]	Grants permission to cancel a response to a message	Write			
CreateConversation [permission only]	Grants permission to create a conversation	Write			
DeleteConversation [permission only]	Grants permission to delete a conversation	Write			
ListConversationMessages [permission only]	Grants permission to list conversation messages	List			
ListConversations [permission only]	Grants permission to list conversations	List			
NotifyConversationIsActive [permission only]	Grants permission to notify whether there is activity in a conversation	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendConversationMessage [permission only]	Grants permission to send a conversation message	Write			

Resource types defined by AWS Network Manager Chat

AWS Network Manager Chat does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Network Manager Chat, specify `"Resource": "*"` in your policy.

Condition keys for AWS Network Manager Chat

Network Manager Chat has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Nimble Studio

Amazon Nimble Studio (service prefix: `nimble`) 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 Nimble Studio

- Resource types defined by Amazon Nimble Studio
- Condition keys for Amazon Nimble Studio

Actions defined by Amazon Nimble Studio

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptEulas	Grants permission to accept EULAs	Write	eula*		
CreateLaunchProfile	Grants permission to create a launch profile	Write	studio*		ec2:CreateNetworkInterface ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeVpcEndpoints ec2:RunInstances
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingImage	Grants permission to create a streaming image	Write	studio*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute ec2:RegisterImage

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSession	Grants permission to create a streaming session	Write	launch-profile*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission nimble:GetLaunchProfile nimble:GetLaunchProfileInitialization nimble:ListEulaAcceptances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateStreamingSessionStream	Grants permission to create a StreamingSessionStream	Write	streaming-session*		
				nimble:requesterPrincipalId	
CreateStudio	Grants permission to create a studio	Write	studio*		iam:PassRole sso:CreateManagedApplicationInstance
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStudioComponent	Grants permission to create a studio component. A studio component designates a network resource to which a launch profile will provide access	Write	studio*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteLaunchProfile	Grants permission to delete a launch profile	Write	launch-profile*		
DeleteLaunchProfileMember	Grants permission to delete a launch profile member	Write	launch-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStreamingImage	Grants permission to delete a streaming image	Write	streaming-image*		ec2:DeleteSnapshot ec2:DeregisterImage ec2:ModifyInstanceAttribute ec2:ModifySnapshotAttribute
DeleteStreamingSession	Grants permission to delete a streaming session	Write	streaming-session*		ec2:DeleteNetworkInterface
				nimble:requesterPrincipalId	
DeleteStudio	Grants permission to delete a studio	Write	studio*		sso:DeleteManagedApplicationInstance
DeleteStudioComponent	Grants permission to delete a studio component	Write	studio-component*		ds:UnauthorizeApplication
DeleteStudioMember	Grants permission to delete a studio member	Write	studio*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEula	Grants permission to get a EULA	Read	eula*		
GetFeatureMap [permission only]	Grants permission to allow Nimble Studio portal to show the appropriate features for this account	Read			
GetLaunchProfile	Grants permission to get a launch profile	Read	launch-profile*		
GetLaunchProfileDetails	Grants permission to get a launch profile's details, which includes the summary of studio components and streaming images used by the launch profile	Read	launch-profile*		
GetLaunchProfileInitialization	Grants permission to get a launch profile initialization. A launch profile initialization is a dereferenced version of a launch profile, including attached studio component connection information	Read	launch-profile*		ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems
GetLaunchProfileMember	Grants permission to get a launch profile member	Read	launch-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStreamingImage	Grants permission to get a streaming image	Read	streaming-image*		
GetStreamingSession	Grants permission to get a streaming session	Read	streaming-session*		
				nimble:requesterPrincipalId	
GetStreamingSessionBackup	Grants permission to get a streaming session backup	Read	streaming-session-backup*		
				nimble:requesterPrincipalId	
GetStreamingSessionStream	Grants permission to get a streaming session stream	Read	streaming-session*		
				nimble:requesterPrincipalId	
GetStudio	Grants permission to get a studio	Read	studio*		
GetStudioComponent	Grants permission to get a studio component	Read	studio-component*		
GetStudioMember	Grants permission to get a studio member	Read	studio*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEulaAcceptances	Grants permission to list EULA acceptances	Read	eula-acceptance*		
ListEulas	Grants permission to list EULAs	Read	eula*		
ListLaunchProfileMembers	Grants permission to list launch profile members	Read	launch-profile*		
ListLaunchProfiles	Grants permission to list launch profiles	Read	studio*		
				nimble:principalId nimble:requesterPrincipalId	
ListStreamingImages	Grants permission to list streaming images	Read	studio*		
ListStreamingSessionBackups	Grants permission to list streaming session backups	Read	studio*		
				nimble:requesterPrincipalId	
ListStreamingSessions	Grants permission to list streaming sessions	Read	studio*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				nimble:createdBy nimble:ownedBy nimble:requesterPrincipalId	
ListStudioComponents	Grants permission to list studio components	Read	studio*		
ListStudioMembers	Grants permission to list studio members	Read	studio*		
ListStudios	Grants permission to list all studios	Read			
ListTagsForResource	Grants permission to list all tags on a Nimble Studio resource	Read	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			studio-component		
PutLaunchProfileMembers	Grants permission to add/update launch profile members	Write	launch-profile*		sso-directory:DescribeUsers
PutStudioLogEvents [permission only]	Grants permission to report metrics and logs for the Nimble Studio portal to monitor application health	Write	studio*		
PutStudioMembers	Grants permission to add/update studio members	Write	studio*		sso-directory:DescribeUsers
StartStreamingSession	Grants permission to start a streaming session	Write	streaming-session*		nimble:GetLaunchProfile nimble:GetLaunchProfileMember
			streaming-session-backup		
				nimble:requesterPrincipalId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartStudioSSOConfigurationRepair	Grants permission to repair the studio's AWS IAM Identity Center configuration	Write	studio*		sso:CreateManagedApplicationInstance sso:GetManagedApplicationInstance
StopStreamingSession	Grants permission to stop a streaming session	Write	streaming-session*		nimble:GetLaunchProfile
				nimble:requesterPrincipalId	
TagResource	Grants permission to add or overwrite one or more tags for the specified Nimble Studio resource	Tagging	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			studio-component		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to disassociate one or more tags from the specified Nimble Studio resource	Tagging	launch-profile		
			streaming-image		
			streaming-session		
			streaming-session-backup		
			studio		
			studio-component		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateLaunchProfile	Grants permission to update a launch profile	Write	launch-profile*		ec2:DescribeNatGateways ec2:DescribeNetworkAcls ec2:DescribeRouteTables ec2:DescribeSubnets ec2:DescribeVpcEndpoints
UpdateLaunchProfileMember	Grants permission to update a launch profile member	Write	launch-profile*		
UpdateStreamingImage	Grants permission to update a streaming image	Write	streaming-image*		
UpdateStudio	Grants permission to update a studio	Write	studio*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStudioComponent	Grants permission to update a studio component	Write	studio-component*		ds:AuthorizeApplication ds:DescribeDirectories ec2:DescribeSecurityGroups fsx:DescribeFileSystems iam:PassRole

Resource types defined by Amazon Nimble Studio

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
studio	`arn:${Partition}:nimble:${Region}:${Account}:studio/${StudioId}`	aws:RequestTag/${TagKey}

Resource types	ARN	Condition keys
		aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
streaming-image	arn:${Partition}:nimble:${Region}:${Account}:streaming-image/${StreamingImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
studio-component	arn:${Partition}:nimble:${Region}:${Account}:studio-component/${StudioComponentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId
launch-profile	arn:${Partition}:nimble:${Region}:${Account}:launch-profile/${LaunchProfileId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:studioId

Resource types	ARN	Condition keys
streaming-session	arn:${Partition}:nimble:${Region}:${Account}:streaming-session/${StreamingSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:createdBy nimble:ownedBy
streaming-session-backup	arn:${Partition}:nimble:${Region}:${Account}:streaming-session-backup/${StreamingSessionBackupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys nimble:ownedBy
eula	arn:${Partition}:nimble:${Region}:${Account}:eula/${EulaId}	
eula-acceptance	arn:${Partition}:nimble:${Region}:${Account}:eula-acceptance/${EulaAcceptanceId}	nimble:studioId

Condition keys for Amazon Nimble Studio

Amazon Nimble Studio defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
nimble:createdBy	Filters access by the createdBy request parameter or the ID of the creator of the resource	String
nimble:ownedBy	Filters access by the ownedBy request parameter or the ID of the owner of the resource	String
nimble:principalId	Filters access by the principalId request parameter	String
nimble:requesterPrincipalId	Filters access by the ID of the logged in user	String
nimble:studioId	Filters access by a specific studio	ARN

Actions, resources, and condition keys for Amazon Nova Act

Amazon Nova Act (service prefix: `nova-act`) 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 Nova Act

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAct	Grants permission to create a new AI task (act) within a session that can interact with tools and perform specific actions	Write	workflow-definition*		
			workflow-run*		
CreateSession	Grants permission to create a new session context within a workflow run to manage conversation state and acts	Write	workflow-definition*		
			workflow-run*		
CreateWorkflowDefinition	Grants permission to create a new workflow definition template that can be used to execute multiple workflow runs	Write	workflow-definition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflowRun	Grants permission to create a new execution instance of a workflow definition with specified parameters	Write	workflow-definition*		
DeleteWorkflowDefinition	Grants permission to delete a workflow definition and all associated resources	Write	workflow-definition*		
DeleteWorkflowRun	Grants permission to terminate and clean up a workflow run, stopping all associated acts and sessions	Write	workflow-definition*		
			workflow-run*		
GetWorkflowDefinition	Grants permission to retrieve details and configuration of a specific workflow definition	Read	workflow-definition*		
GetWorkflowRun	Grants permission to retrieve the current state, configuration, and execution details of a workflow run	Read	workflow-definition*		
			workflow-run*		
InvokeActStep	Grants permission to execute the next step of an act, processing tool call results and returning new tool calls if needed	Write	workflow-definition*		
			workflow-run*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListActs	Grants permission to list all acts within a specific session with their current status and execution details	Read	workflow-definition*		
ListModels	Grants permission to list all available AI models that can be used for workflow execution, including their status and compatibility information	Read			
ListSessions	Grants permission to list all sessions within a specific workflow run	Read	workflow-definition*		
			workflow-run*		
ListWorkflowDefinitions	Grants permission to list all workflow definitions in your account with optional filtering and pagination	List			
ListWorkflowRuns	Grants permission to list all workflow runs for a specific workflow definition with optional filtering and pagination	List	workflow-definition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAct	Grants permission to update an existing act's configuration, status, or error information	Write	workflow-definition*		
			workflow-run*		
UpdateWorkflowRun	Grants permission to update the configuration or state of an active workflow run	Write	workflow-definition*		
			workflow-run*		

Resource types defined by Amazon Nova Act

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
workflow-definition	`arn:${Partition}:nova-act:${Region}:${Account}:workflow-definition/${WorkflowDefinitionName}`	
workflow-run	`arn:${Partition}:nova-act:${Region}:${Account}:workflow-definition/${Wor`	

Resource types	ARN	Condition keys
	kflowDefinitionName}/workflow-run/${ WorkflowRunId}	

Condition keys for Amazon Nova Act

Nova Act has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon One Enterprise

Amazon One Enterprise (service prefix: one) 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 One Enterprise
- Resource types defined by Amazon One Enterprise
- Condition keys for Amazon One Enterprise

Actions defined by Amazon One Enterprise

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDeviceActivationQrCode	Grants permission to create a QR code for a Device Instance	Write	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateDeviceConfigurationTemplate	Grants permission to create a Device Configuration Template	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstance	Grants permission to create a Device Instance	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceInstanceConfiguration	Grants permission to create a Device Instance Configuration	Write	device-instance*		
				aws:ResourceTag/${TagKey}	
CreateSite	Grants permission to create a Site	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
DeleteAssociatedDevice	Grants permission to disassociate Device from a Device Instance	Write	device-instance*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceConfigurationTemplate	Grants permission to delete a Device Configuration Template	Write	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
DeleteDeviceInstance	Grants permission to delete a Device Instance	Write	device-instance*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSite	Grants permission to delete a Site	Write	site*		
				aws:ResourceTag/${TagKey}	
DeleteUserV1	Grants permission to delete a User	Write	user*		
GetDeviceConfigurationTemplate	Grants permission to view a Device Configuration Template	Read	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstance	Grants permission to view a Device Instance	Read	device-instance*		
				aws:ResourceTag/${TagKey}	
GetDeviceInstanceConfiguration	Grants permission to view a Device Instance Configuration	Read	configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetSite	Grants permission to view a Site	Read	site*		
				aws:ResourceTag/${TagKey}	
GetSiteAddress	Grants permission to view address of a Site	Read	site*		
				aws:ResourceTag/${TagKey}	
ListDeviceConfigurationTemplates	Grants permission to retrieve list of Device Configuration Templates	List			
ListDeviceInstances	Grants permission to retrieve list of Device Instances	List			
ListSites	Grants permission to view list of Sites	List			
ListTagsForResource	Grants permission to list tags for an Amazon One Enterprise resource	Read	device-configuration-template		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			device-instance		
			site		
				aws:ResourceTag/${TagKey}	
ListUsers	Grants permission to view list of Users	List			
ListUsersV1	Grants permission to view list of Users	List			
RebootDevice	Grants permission to reboot Device associated with a Device Instance	Write	device-instance*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to add tags to an Amazon One Enterprise resource	Tagging	device-configuration-template		
			device-instance		
			site		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from an Amazon One Enterprise resource	Tagging	device-configuration-template		
			device-instance		
			site		
				aws:TagKeys	
UpdateDeviceConfigurationTemplate	Grants permission to update a Device Configuration Template	Write	device-configuration-template*		
				aws:ResourceTag/${TagKey}	
UpdateDeviceInstance	Grants permission to update a Device Instance	Write	device-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateSite	Grants permission to update a Site	Write	site*		
				aws:ResourceTag/${TagKey}	
UpdateSiteAddress	Grants permission to update address of a Site	Write	site*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon One Enterprise

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-instance	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}	aws:ResourceTag/${TagKey}
configuration	arn:${Partition}:one:${Region}:${Account}:device-instance/${DeviceInstanceId}/configuration/${Version}	
device-configuration-template	arn:${Partition}:one:${Region}:${Account}:device-configuration-template/${TemplateId}	aws:ResourceTag/${TagKey}
site	arn:${Partition}:one:${Region}:${Account}:site/${SiteId}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:one:${Region}:${Account}:user/${UserId}	

Condition keys for Amazon One Enterprise

Amazon One Enterprise defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by using tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by using 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 OpenSearch

Amazon OpenSearch (service prefix: `opensearch`) 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
- Resource types defined by Amazon OpenSearch
- Condition keys for Amazon OpenSearch

Actions defined by Amazon OpenSearch

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApplicationAccessAll [permission only]	Grants permission to access OpenSearch Application	Permissions management	application*		
CancelAutoOptimizeJob	Grants permission to cancel submitted Auto Optimize Job	Write			
CancelDirectQuery	Grants permission to cancel the query that is submitted on the OpenSearch DataSource resource	Write	datasource*		
DeleteAutoOptimizeJob	Grants permission to delete Auto Optimize Job	Write			
GetAutoOptimizeJob	Grants permission to get the Auto Optimize Job details	Read			
GetDirectQuery	Grants permission to get the query status that are performed on the OpenSearch DataSource resource	Read	datasource*		
GetDirectQueryResult	Grants permission to get the results of a query that is performed on the OpenSearch DataSource resource	Read	datasource*		
ListAutoOptimizeJobs	Grants permission to retrieve a list of Auto Optimize Jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDirectQuery	Grants permission to start a direct query on the provided OpenSearch DataSource arns	Write	datasource*		
SubmitAutoOptimizeJob	Grants permission to create new Auto Optimize Job	Write			

Resource types defined by Amazon OpenSearch

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:${Partition}:opensearch:${Region}:${Account}:application/${AppId}`	
datasource	`arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}`	

Condition keys for Amazon OpenSearch

OpenSearch has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion (service prefix: `osis`) 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 Ingestion

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePipeline	Grants permission to create an OpenSearch Ingestion pipeline	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:GenerateDataKeyWithoutPlaintext logs:CreateLogDelivery
CreatePipelineEndpoint	Grants permission to create an OpenSearch Ingestion pipeline endpoint	Write	pipeline*		iam:CreateServiceLinkedRole
				aws:TagKeys aws:RequestTag/${TagKey}	
DeletePipeline	Grants permission to delete an OpenSearch Ingestion pipeline	Write	pipeline*		logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePipelineEndpoint	Grants permission to delete an OpenSearch Ingestion pipeline endpoint in the current account	Write	pipeline-endpoint*		
DeleteResourcePolicy	Grants permission to delete a resource policy for an OpenSearch Ingestion resource	Write	pipeline*		
GetPipeline	Grants permission to retrieve configuration information for an OpenSearch Ingestion pipeline	Read	pipeline*		
GetPipelineBlueprint	Grants permission to get the contents of an OpenSearch Ingestion pipeline blueprint	Read	pipeline-blueprint*		
GetPipelineChangeProgress	Grants permission to get granular information about the status of an OpenSearch Ingestion pipeline	Read	pipeline*		
GetResourcePolicy	Grants permission to get a resource policy for an OpenSearch Ingestion resource	Read	pipeline*		
Ingest	Grants permission to ingest data through an OpenSearch Ingestion pipeline	Write	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPipelineBlueprints	Grants permission to list the names of available blueprints for an OpenSearch Ingestion pipeline configuration	List			
ListPipelineEndpointConnections	Grants permission to list OpenSearch Ingestion pipeline endpoint connections to pipelines in the current account	List			
ListPipelineEndpoints	Grants permission to list OpenSearch Ingestion pipeline endpoints in the current account	List			
ListPipelines	Grants permission to list basic configuration for each OpenSearch Ingestion pipeline in the current account and Region	List			
ListTagsForResource	Grants permission to list all resource tags associated with an OpenSearch Ingestion pipeline	Read	pipeline*		
PutResourcePolicy	Grants permission to put a resource policy for an OpenSearch Ingestion resource	Write	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokePipelineEndpointConnections	Grants permission to revoke an OpenSearch Ingestion pipeline endpoint connection from a pipeline in the current account	Write	pipeline*		
StartPipeline	Grants permission to start an OpenSearch Ingestion pipeline	Write	pipeline*		
StopPipeline	Grants permission to stop an OpenSearch Ingestion pipeline	Write	pipeline*		
TagResource	Grants permission to attach resource tags to an OpenSearch Ingestion pipeline	Tagging	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove resource tags from an OpenSearch Ingestion Service pipeline	Tagging	pipeline*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePipeline	Grants permission to modify the configuration of an OpenSearch Ingestion pipeline	Write	pipeline*		iam:PassRole kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
ValidatePipeline	Grants permission to validate the configuration of an OpenSearch Ingestion pipeline	Read			

Resource types defined by Amazon OpenSearch Ingestion

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
pipeline	`arn:${Partition}:osis:${Region}:${Account}:pipeline/${PipelineName}`	aws:ResourceTag/${TagKey}
pipeline-endpoint	`arn:${Partition}:osis:${Region}:${Account}:endpoint/${EndpointId}`	aws:ResourceTag/${TagKey}
pipeline-blueprint	`arn:${Partition}:osis:${Region}:${Account}:blueprint/${BlueprintName}`	

Condition keys for Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon OpenSearch Serverless

Amazon OpenSearch Serverless (service prefix: `aoss`) 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 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
APIAccessAll	Grant permission to all the supported Opensearch APIs	Write	Collection*		
				aoss:collection aoss:CollectionId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddCollectionToCollectionGroup	Grants permission to add a serverless collection to a specified collection group	Write	CollectionGroup*		
				aoss:collection-group	
BatchGetCollection	Grants permission to get attributes for one or more collections	Read		aoss:collection	
BatchGetCollectionGroup	Grants permission to get attributes for one or more collection groups	Read		aoss:collection-group	
BatchGetEffectiveLifecyclePolicy	Grants permission to get the information about a lifecycle policy applied to one or more AOSS resources	Read			
BatchGetLifecyclePolicy	Grants permission to get information about one or more lifecycle policies	Read			
BatchGetVpcEndpoint	Grants permission to get attributes for one or more VPC endpoints	Read			
CreateAccessPolicy	Grants permission to create a data access policy	Write		aoss:collection aoss:index	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCollection	Grants permission to create a serverless collection	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCollectionGroup	Grants permission to create a serverless collection group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIndex	Grants permission to create an opensearch index	Write			
CreateLifecyclePolicy	Grants permission to create a lifecycle policy	Write		aoss:index	
CreateSecurityConfig	Grants permission to create a serverless security configuration	Write			
CreateSecurityPolicy	Grants permission to create a network or encryption policy	Write		aoss:collection	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEndpoint	Grants permission to create an OpenSearch-Serverless-managed interface VPC endpoint	Write			
DashboardsAccessAll	Grants permission to Opensearch Serverless Dashboards	Write	Dashboards*		
				aoss:collection aoss:CollectionId	
DeleteAccessPolicy	Grants permission to delete a data access policy	Write		aoss:collection aoss:index	
DeleteCollection	Grants permission to delete a serverless collection	Write	Collection*		
DeleteCollectionGroup	Grants permission to delete a serverless collection group	Write	CollectionGroup*		
DeleteIndex	Grants permission to delete an opensearch index	Write			
DeleteLifecyclePolicy	Grants permission to delete a lifecycle policy	Write		aoss:index	
DeleteSecurityConfig	Grants permission to delete a security configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSecurityPolicy	Grants permission to delete a security policy	Write		aoss:collection	
DeleteVpcEndpoint	Grants permission to delete an OpenSearch Serverless-managed interface VPC endpoint	Write			
GetAccessPolicy	Grants permission to get information about a data access policy	Read		aoss:collection aoss:index	
GetAccountSettings	Grants permission to get account settings, including capacity settings	Read			
GetIndex	Grants permission to get an opensearch index	Read			
GetPoliciesStats	Grants permission to get statistis about the security policies in your account	Read			
GetSecurityConfig	Grants permission to get information about a serverless security configuration	Read			
GetSecurityPolicy	Grants permission to get information about a security policy	Read		aoss:collection	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPolicies	Grants permission to list data access policies	List			
ListCollectionGroups	Grants permission to list collection groups	List			
ListCollections	Grants permission to list collections	List			
ListLifecyclePolicies	Grants permission to list lifecycle policies	List			
ListSecurityConfigs	Grants permission to list security configurations	List			
ListSecurityPolicies	Grants permission to list security policies	List			
ListTagsForResource	Grants permission to list tags for a collection	List			
ListVpcEndpoints	Grants permission to list OpenSearch Serverless-managed VPC endpoints	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a serverless collection	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a collection	Write		aws:TagKeys	
UpdateAccessPolicy	Grants permission to update a data access policy	Write		aoss:collection aoss:index	
UpdateAccountSettings	Grants permission to update account settings, including capacity settings	Write			
UpdateCollection	Grants permission to update a collection	Write	Collection*		
UpdateCollectionGroup	Grants permission to update a collection group	Write	CollectionGroup*		
UpdateIndex	Grants permission to update an opensearch index	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLifecyclePolicy	Grants permission to update a lifecycle policy	Write		aoss:index	
UpdateSecurityConfig	Grants permission to update a security configuration	Write			
UpdateSecurityPolicy	Grants permission to update a security policy	Write		aoss:collection	
UpdateVpcEndpoint	Grants permission to update an OpenSearch Serverless-managed VPC endpoint	Write			

Resource types defined by Amazon OpenSearch 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
Collection	`arn:${Partition}:aoss:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
CollectionGroup	`arn:${Partition}:aoss:${Region}:${Account}:collection-group/${CollectionGroupId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Dashboards	`arn:${Partition}:aoss:${Region}:${Account}:dashboards/default`	

Condition keys for Amazon OpenSearch Serverless

Amazon OpenSearch 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 AWS global condition context keys.

Condition keys	Description	Type
aoss:CollectionId	Filters access by the identifier of the collection	String
aoss:collection	Filters access by the collection name	String
aoss:collection-group	Filters access by the collection group name	String
aoss:index	Filters access by the index	String
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 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptInboundConnection	Grants permission to the destination domain owner to accept an inbound cross-cluster search connection request	Write			
AcceptInboundCrossClusterSe	Grants permission to the destination domain owner to accept an inbound cross-cluster search connection	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
archConnection	request. This permission is deprecated. Use AcceptInboundConnection instead				
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociatePackage	Grants permission to associate a package with an OpenSearch Service domain	Write	domain*		
AssociatePackages	Grants permission to associate multiple packages with an OpenSearch Service domain	Write	domain*		
AuthorizeVpcEndpointAccess	Grants permission to provide access to an Amazon OpenSearch Service domain through the use of an interface VPC endpoint	Write			
CancelDomainConfigChange	Grants permission to cancel a change on an OpenSearch Service domain	Write	domain*		
CancelElasticsearchServiceSoftwareUpdate	Grants permission to cancel a service software update of a domain. This permission is deprecated. Use CancelServiceSoftwareUpdate instead	Write	domain*		
CancelServiceSoftwareUpdate	Grants permission to cancel a service software update of a domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an OpenSearch Application	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Grants permission to create an Amazon OpenSearch Service domain	Write	domain		
				aws:RequestTag/${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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateElasticsearchServiceRole	Grants permission to create the service-linked role required for OpenSearch Service domains that use VPC access. This permission is deprecated. OpenSearch Service creates the service-linked role for you	Write			
CreateIndex	Grants permission to create index for the OpenSearch Service domain	Write	domain*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DeleteInboundCrossClusterSearchConnection	Grants permission to the destination domain owner to delete an existing inbound cross-cluster search connection. This permission is deprecated. Use DeleteInboundConnection instead	Write			
DeleteIndex	Grants permission to delete Index for the OpenSearch Service domain	Write	domain*		
DeleteOutboundConnection	Grants permission to the source domain owner to delete an existing outbound cross-cluster search connection	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeInboundCrossClusterSearchConnections	Grants permission to list all the inbound cross-cluster search connections for a destination domain. This permission is deprecated. Use DescribeInboundConnections instead	List			
DescribeInsightDetails	Grants permission to view detailed information about insights for an OpenSearch Service domain	Read	domain*		
DescribeInstanceTypeLimits	Grants permission to view the instance count, storage, and master node limits for a given engine version and instance type	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetDefaultApplicationSetting	Grants permission to get the default application setting for OpenSearch Service	Read	application*		
GetDirectQueryDataSource	Grants permission to get the data source for the provided OpenSearch arns	Read	datasource*		
GetDomainMaintenanceStatus	Grants permission to retrieve the status of maintenance action for the node	Read	domain*		
GetIndex	Grants permission to get index for the OpenSearch Service domain	Read	domain*		
GetPackageVersionHistory	Grants permission to fetch the version history for a package	Read			
GetUpgradeHistory	Grants permission to fetch the upgrade history of a given OpenSearch Service domain	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListInsights	Grants permission to list insights for OpenSearch Service domains in the account	List	domain		
ListInstanceTypeDetails	Grants permission to list all instance types and available features for a given OpenSearch or Elasticsearch version	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListVpcEndpointAccess	Grants permission to retrieve information about each AWS principal that is allowed to access a given Amazon OpenSearch Service domain through the use of an interface VPC endpoint	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVpcEndpoints	Grants permission to retrieve all Amazon OpenSearch Service-managed VPC endpoints in the current AWS account and Region	List			
ListVpcEndpointsForDomain	Grants permission to retrieve all Amazon OpenSearch Service-managed VPC endpoints associated with a particular domain	List			
PurchaseReservedElasticsearchInstanceOffering	Grants permission to purchase OpenSearch Service Reserved Instances. This permission is deprecated. Use PurchaseReservedInstanceOffering instead	Write			
PurchaseReservedInstanceOffering	Grants permission to purchase OpenSearch reserved instances	Write			
PutDefaultApplicationSetting	Grants permission to set or remove the default application setting for OpenSearch Service	Write	application*		

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
RollbackElasticsearchServiceSoftwareUpdate	Grants permission to rollback a service software update of an elasticsearch domain to its previous version	Write	domain*		
RollbackServiceSoftwareUpdate	Grants permission to rollback a service software update of an opensearch domain to its previous version	Write	domain*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateElasticsearchDomainConfig	Grants permission to modify the configuration of an OpenSearch Service domain, such as the instance type or number of instances. This permission is deprecated. Use UpdateDomainConfig instead	Write	domain*		
UpdateIndex	Grants permission to update index for the OpenSearch Service domain	Write	domain*		
UpdatePackage	Grants permission to update a package for use with OpenSearch Service domains	Write			
UpdatePackageScope	Grants permission to update scope a package	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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::${Account}:role/aws-service-role/opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService	aws:ResourceTag/${TagKey}
datasource	arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon OpenSearch Service

Amazon OpenSearch Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS OpsWorks

AWS OpsWorks (service prefix: `opsworks`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS OpsWorks
- Resource types defined by AWS OpsWorks
- Condition keys for AWS OpsWorks

Actions defined by AWS OpsWorks

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignInstance	Grants permission to assign a registered instance to a layer	Write	stack		
AssignVolume	Grants permission to assign one of the stack's registered Amazon EBS volumes to a specified instance	Write	stack		
AssociateElasticIp	Grants permission to associate one of the stack's registered Elastic IP addresses with a specified instance	Write	stack		
AttachElasticLoadBalancer	Grants permission to attach an Elastic Load Balancing load balancer to a specified layer	Write	stack		
CloneStack	Grants permission to create a clone of a specified stack	Write	stack		
CreateApp	Grants permission to create an app for a specified stack	Write	stack		
CreateDeployment	Grants permission to run deployment or stack commands	Write	stack		
CreateInstance	Grants permission to create an instance in a specified stack	Write	stack		
CreateLayer	Grants permission to create a layer	Write	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStack	Grants permission to create a new stack	Write			
CreateUserProfile	Grants permission to create a new user profile	Write			
DeleteApp	Grants permission to delete a specified app	Write	stack		
DeleteInstance	Grants permission to delete a specified instance, which terminates the associated Amazon EC2 instance	Write	stack		
DeleteLayer	Grants permission to delete a specified layer	Write	stack		
DeleteStack	Grants permission to delete a specified stack	Write	stack		
DeleteUserProfile	Grants permission to delete a user profile	Write			
DeregisterEcsCluster	Grants permission to delete a user profile	Write	stack		
DeregisterElasticIp	Grants permission to deregister a specified Elastic IP address	Write	stack		
DeregisterInstance	Grants permission to deregister a registered Amazon EC2 or on-premises instance	Write	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterRdsDbInstance	Grants permission to deregister an Amazon RDS instance	Write	stack		
DeregisterVolume	Grants permission to deregister an Amazon EBS volume	Write	stack		
DescribeAgentVersions	Grants permission to describe the available AWS OpsWorks agent versions	List	stack		
DescribeApps	Grants permission to request a description of a specified set of apps	List	stack		
DescribeCommands	Grants permission to describe the results of specified commands	List	stack		
DescribeDeployments	Grants permission to request a description of a specified set of deployments	List	stack		
DescribeEcsClusters	Grants permission to describe Amazon ECS clusters that are registered with a stack	List	stack		
DescribeElasticIps	Grants permission to describe Elastic IP addresses	List	stack		
DescribeElasticLoadBalancers	Grants permission to describe a stack's Elastic Load Balancing instances	List	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstances	Grants permission to request a description of a set of instances	List	stack		
DescribeLayers	Grants permission to request a description of one or more layers in a specified stack	List	stack		
DescribeLoadBasedAutoScaling	Grants permission to describe load-based auto scaling configurations for specified layers	List	stack		
DescribeMyUserProfile	Grants permission to describe a user's SSH information	List			
DescribeOperatingSystems	Grants permission to describe the operating systems that are supported by AWS OpsWorks Stacks	List			
DescribePermissions	Grants permission to describe the permissions for a specified stack	List	stack		
DescribeRaidArrays	Grants permission to describe an instance's RAID arrays	List	stack		
DescribeRdsDbInstances	Grants permission to describe Amazon RDS instances	List	stack		
DescribeServiceErrors	Grants permission to describe AWS OpsWorks service errors	List	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStackProvisioningParameters	Grants permission to request a description of a stack's provisioning parameters	List	stack		
DescribeStackSummary	Grants permission to describe the number of layers and apps in a specified stack, and the number of instances in each state, such as running_setup or online	List	stack		
DescribeStacks	Grants permission to request a description of one or more stacks	List	stack		
DescribeTimeBasedAutoScaling	Grants permission to describe time-based auto scaling configurations for specified instances	List	stack		
DescribeUserProfiles	Grants permission to describe specified users	List			
DescribeVolumes	Grants permission to describe an instance's Amazon EBS volumes	List	stack		
DetachElasticLoadBalancer	Grants permission to detache a specified Elastic Load Balancing instance from its layer	Write	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateElasticIp	Grants permission to disassociate an Elastic IP address from its instance	Write	stack		
GetHostnameSuggestion	Grants permission to get a generated host name for the specified layer, based on the current host name theme	Read	stack		
GrantAccess	Grants permission to grant RDP access to a Windows instance for a specified time period	Write	stack		
ListTags	Grants permission to return a list of tags that are applied to the specified stack or layer	List	stack		
RebootInstance	Grants permission to reboot a specified instance	Write	stack		
RegisterEcsCluster	Grants permission to register a specified Amazon ECS cluster with a stack	Write	stack		
RegisterElasticIp	Grants permission to register an Elastic IP address with a specified stack	Write	stack		
RegisterInstance	Grants permission to register instances with a specified stack that were created outside of AWS OpsWorks	Write	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterRdsDbInstance	Grants permission to register an Amazon RDS instance with a stack	Write	stack		
RegisterVolume	Grants permission to register an Amazon EBS volume with a specified stack	Write	stack		
SetLoadBasedAutoScaling	Grants permission to specify the load-based auto scaling configuration for a specified layer	Write	stack		
SetPermission	Grants permission to specify a user's permissions	Permissions management	stack		
SetTimeBasedAutoScaling	Grants permission to specify the time-based auto scaling configuration for a specified instance	Write	stack		
StartInstance	Grants permission to start a specified instance	Write	stack		
StartStack	Grants permission to start a stack's instances	Write	stack		
StopInstance	Grants permission to stop a specified instance	Write	stack		
StopStack	Grants permission to stop a specified stack	Write	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to apply tags to a specified stack or layer	Tagging	stack		
UnassignInstance	Grants permission to unassign a registered instance from all of it's layers	Write	stack		
UnassignVolume	Grants permission to unassign an assigned Amazon EBS volume	Write	stack		
UntagResource	Grants permission to remove tags from a specified stack or layer	Tagging	stack		
UpdateApp	Grants permission to update a specified app	Write	stack		
UpdateElasticIp	Grants permission to update a registered Elastic IP address's name	Write	stack		
UpdateInstance	Grants permission to update a specified instance	Write	stack		
UpdateLayer	Grants permission to update a specified layer	Write	stack		
UpdateMyUserProfile	Grants permission to update a user's SSH public key	Write			
UpdateRdsDbInstance	Grants permission to update an Amazon RDS instance	Write	stack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStack	Grants permission to update a specified stack	Write	stack		
UpdateUserProfile	Grants permission to update a specified user profile	Permissions management			
UpdateVolume	Grants permission to update an Amazon EBS volume's name or mount point	Write	stack		

Resource types defined by AWS OpsWorks

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
stack	`arn:${Partition}:opsworks:${Region}:${Account}:stack/${StackId}/`	

Condition keys for AWS OpsWorks

OpsWorks has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS OpsWorks Configuration Management

AWS OpsWorks Configuration Management (service prefix: `opsworks-cm`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS OpsWorks Configuration Management

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateNode	Grants permission to associate a node to a configuration management server	Write			
CreateBackup	Grants permission to create a backup for the specified server	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServer	Grants permission to create a new server	Write			
DeleteBackup	Grants permission to delete the specified backup and possibly its S3 bucket	Write			
DeleteServer	Grants permission to delete the specified server with its corresponding CloudFormation stack and possibly the S3 bucket	Write			
DescribeAccountAttributes	Grants permission to describe the service limits for the user's account	List			
DescribeBackups	Grants permission to describe a single backup, all backups of a specified server or all backups of the user's account	List			
DescribeEvents	Grants permission to describe all events of the specified server	List			
DescribeNodeAssociationStatus	Grants permission to describe the association status for the specified node token and the specified server	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServers	Grants permission to describe the specified server or all servers of the user's account	List			
DisassociateNode	Grants permission to disassociate a specified node from a server	Write			
ExportServerEngineAttribute	Grants permission to export an engine attribute from a server	Read			
ListTagsForResource	Grants permission to list the tags that are applied to the specified server or backup	Read			
RestoreServer	Grants permission to apply a backup to specified server. Possibly swaps out the ec2-instance if specified	Write			
StartMaintenance	Grants permission to start the server maintenance immediately	Write			
TagResource	Grants permission to apply tags to the specified server or backup	Tagging			
UntagResource	Grants permission to remove tags from the specified server or backup	Tagging			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServer	Grants permission to update general server settings	Write			
UpdateServerEngineAttributes	Grants permission to update server settings specific to the configuration management type	Write			

Resource types defined by AWS OpsWorks Configuration 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
server	`arn:${Partition}:opsworks-cm::${Account}:server/${ServerName}/${UniqueId}`	
backup	`arn:${Partition}:opsworks-cm::${Account}:backup/${ServerName}-{Date-and-Time-Stamp-of-Backup}`	

Condition keys for AWS OpsWorks Configuration Management

OpsworksCM has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Organizations

AWS Organizations (service prefix: `organizations`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Organizations
- Resource types defined by AWS Organizations
- Condition keys for AWS Organizations

Actions defined by AWS Organizations

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptHandshake	Grants permission to send a response to the originator of a handshake agreeing to the action proposed by the handshake request	Write	handshake*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachPolicy	Grants permission to attach a policy to a root, an organizational unit, or an individual account	Write	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
CancelHandshake	Grants permission to cancel a handshake	Write	handshake*		
CloseAccount	Grants permission to close an AWS account that is now a part of an Organizations, either created within the organization, or invited to join the organization	Write	account*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccount	Grants permission to create an AWS 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 AWS 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 AWS account	Write		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeclineHandshake	Grants permission to decline a handshake request. This sets the handshake state to DECLINED and effectively deactivates the request	Write	handshake*		
DeleteOrganization	Grants permission to delete the organization	Write			
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 AWS account as a delegated administrator for the AWS service that is specified by ServicePrincipal	Write	account*		
				organizations:ServicePrincipal	
DescribeAccount	Grants permission to retrieve Organizations-related details about the specified account	Read	account*		
DescribeCreateAccountStatus	Grants permission to retrieve the current status of an asynchronous request to create an account	Read			
DescribeEffectivePolicy	Grants permission to retrieve the effective policy for an account	Read	account*		
				organizations:PolicyType	
DescribeHandshake	Grants permission to retrieve details about a previously requested handshake	Read	handshake*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrganization	Grants permission to retrieve details about the organization that the calling credentials belong to	Read			
DescribeOrganizationalUnit	Grants permission to retrieve details about an organizational unit (OU)	Read	organizationalunit*		
DescribePolicy	Grants permission to retrieve details about a policy	Read	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Grants permission to retrieve information about a resource policy	Read			
DescribeResponsibilityTransfer	Grants permission to retrieve details about a previously responsibility transfer	Read	responsibilitytransfer*		
				organizations:TransferType organizations:TransferDirection	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachPolicy	Grants permission to detach a policy from a target root, organizational unit, or account	Write	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	Grants permission to disable integration of an AWS service (the service that is specified by ServicePrincipal) with AWS Organizations	Write		organizations:ServicePrincipal	
DisablePolicyType	Grants permission to disable an organization policy type in a root	Write	root*		
				organizations:PolicyType	
EnableAWSServiceAccess	Grants permission to enable integration of an AWS service (the service that is specified by ServicePrincipal) with AWS Organizations	Write		organizations:ServicePrincipal	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableAllFeatures	Grants permission to start the process to enable all features in an organization, upgrading it from supporting only Consolidated Billing features	Write			
EnablePolicyType	Grants permission to enable a policy type in a root	Write	root*		
				organizations:PolicyType	
InviteAccountToOrganization	Grants permission to send an invitation to another AWS account, asking it to join your organization as a member account	Write	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
InviteOrganizationToTransferResponsibility	Grants permission to send an invitation to another AWS account, asking it to transfer a particular responsibility to your organization	Write	account		
				organizations:TransferType organizations:TransferDirection	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LeaveOrganization	Grants permission to remove a member account from its parent organization	Write			
ListAWSServiceAccessForOrganization	Grants permission to retrieve the list of the AWS services for which you enabled integration with your organization	List			
ListAccounts	Grants permission to list all of the accounts in the organization	List			
ListAccountsForParent	Grants permission to list the accounts in an organization that are contained by a root or organizational unit (OU)	List	organizationalunit		
			root		
ListAccountsWithInvalidEffectivePolicy	Grants permission to list accounts that have invalid effective policies for a specified policy type	List		organizations:PolicyType	
ListChildren	Grants permission to list all of the OUs or accounts that are contained in a parent OU or root	List	organizationalunit		
			root		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCreateAccountStatus	Grants permission to list the asynchronous account creation requests that are currently being tracked for the organization	List			
ListDelegatedAdministrators	Grants permission to list the AWS accounts that are designated as delegated administrators in this organization	List		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	Grants permission to list the AWS services for which the specified account is a delegated administrator in this organization	List	account*		
ListEffectivePolicyValidationErrors	Grants permission to list validation errors found in the effective policy for a specific account and policy type	List	account*		
				organizations:PolicyType	
ListHandshakesForAccount	Grants permission to list all of the handshakes that are associated with an account	List			
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
ListInboundResponsibilityTransfers	Grants permission to list all responsibilities of a particular type transfered to your organization	List		organizations:TransferType organizations:TransferDirection	
ListOrganizationalUnitsForParent	Grants permission to list all of the organizational units (OUs) in a parent organizational unit or root	List	organizationalunit		
			root		
ListOutboundResponsibilityTransfers	Grants permission to list all responsibilities of a particular type transfered to another organization	List		organizations:TransferType organizations:TransferDirection	
ListParents	Grants permission to list the root or organizational units (OUs) that serve as the immediate parent of a child OU or account	List	account		
			organizationalunit		
ListPolicies	Grants permission to list all of the policies in an organization	List		organizations:PolicyType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPoliciesForTarget	Grants permission to list all of the policies that are directly attached to a root, organizational unit (OU), or account	List	account		
			organizationalunit		
			root		
				organizations:PolicyType	
ListRoots	Grants permission to list all of the roots that are defined in the organization	List			
ListTagsForResource	Grants permission to list all tags for the specified resource	List	account		
			organizationalunit		
			policy		
			resourcepolicy		
			responsibilitytransfer	organizations:TransferType	
				organizations:TransferDirection	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			root		
				organizations:PolicyType	
ListTargetsForPolicy	Grants permission to list all the roots, OUs, and accounts to which a policy is attached	List	policy*		
				organizations:PolicyType	
MoveAccount	Grants permission to move an account from its current root or OU to another parent root or OU	Write	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	Grants permission to create or update a resource policy	Write	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterDelegatedAdministrator	Grants permission to register the specified member account to administer the Organizations features of the AWS service that is specified by ServicePrincipal	Write	account*		
				organizations:ServicePrincipal	
RemoveAccountFromOrganization	Grants permission to remove the specified account from the organization	Write	account*		
TagResource	Grants permission to add one or more tags to the specified resource	Tagging	account		
			organizationalunit		
			policy	organizations:PolicyType	
			resourcepolicy		
			responsibilitytransfer	organizations:TransferType organizations:TransferDirection	
			root		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} organizations:PolicyType	
TerminateResponsibilityTransfer	Grants permission to end the transfer for a responsibility to or from your organization	Write	responsibilitytransfer*		
				organizations:TransferType organizations:TransferDirection	
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	account		
			organizationalunit		
			policy		
			resourcepolicy		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			responsibilitytransfer	organizations:TransferType organizations:TransferDirection	
			root		
				aws:TagKeys organizations:PolicyType	
UpdateOrganizationalUnit	Grants permission to rename an organizational unit (OU)	Write	organizationalunit*		
UpdatePolicy	Grants permission to update an existing policy with a new name, description, or content	Write	policy*		
				organizations:PolicyType	
UpdateResponsibilityTransfer	Grants permission to rename a responsibility transfer to or from your organization	Write	responsibilitytransfer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:TransferType organizations:TransferDirection	

Resource types defined by AWS Organizations

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
account	`arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}`	aws:ResourceTag/${TagKey}
handshake	`arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	
organization	`arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}`	

Resource types	ARN	Condition keys
organizationalunit	arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}	aws:ResourceTag/${TagKey}
resourcepolicy	arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}	aws:ResourceTag/${TagKey}
awspolicy	arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}	
root	arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}	aws:ResourceTag/${TagKey}
responsibilitytransfer	arn:${Partition}:organizations::${Account}:transfer/o-${OrganizationId}/${TransferType}/${TransferDirection}/rt-${ResponsibilityTransferId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Organizations

AWS Organizations defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
organizations:PolicyType	Filters access by the specified policy type names	String
organizations:ServicePrincipal	Filters access by the specified service principal names	String
organizations:TransferDirection	Filters access by the specified responsibility transfer by the direction	String
organizations:TransferType	Filters access by the specified responsibility transfer type names	String

Actions, resources, and condition keys for AWS Outposts

AWS Outposts (service prefix: `outposts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Outposts

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelCapacityTask	Grants permission to cancel a capacity task	Write	outpost*		
CancelOrder	Grants permission to cancel an order	Write			
CreateOrder	Grants permission to create an order	Write	outpost*		
CreateOutpost	Grants permission to create an Outpost	Write	site*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePrivateConnectivityConfig	Grants permission to create a private connectivity configuration	Write	outpost*		
CreateSite	Grants permission to create a site	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteOutpost	Grants permission to delete an Outpost	Write	outpost*		
DeleteSite	Grants permission to delete a site	Write	site*		
GetCapacityTask	Grants permission to get information about the specified capacity task	Read	outpost*		
GetCatalogItem	Grants permission to get a catalog item	Read			
GetConnection	Grants permission to get information about the connection for your Outpost server	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOrder	Grants permission to get information about an order	Read			
GetOutpost	Grants permission to get information about the specified Outpost	Read	outpost*		
GetOutpostBillingInformation	Grants permission to get Outpost billing information for the specified Outpost	Read	outpost*		
GetOutpostInstanceTypes	Grants permission to get the instance types for the specified Outpost	Read	outpost*		
GetOutpostSupportedInstanceTypes	Grants permission to get the supported instance types for the specified Outpost	Read	outpost*		
GetPrivateConnectivityConfig	Grants permission to get a private connectivity configuration	Read	outpost*		
GetSite	Grants permission to get a site	Read	site*		
GetSiteAddress	Grants permission to get a site address	Read	site*		
ListAssetInstances	Grants permission to list all running instances for the specified Outpost	List	outpost*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssets	Grants permission to list the assets for your Outpost	List	outpost*		
ListBlockingInstancesForCapacityTask	Grants permission to list all running instances that are blocking the capacity task from running for the specified Outpost	List	outpost*		
ListCapacityTasks	Grants permission to list the capacity tasks for your AWS account	List			
ListCatalogItems	Grants permission to list all catalog items	List			
ListOrders	Grants permission to list the orders for your AWS account	List			
ListOutposts	Grants permission to list the Outposts for your AWS account	List			
ListSites	Grants permission to list the sites for your AWS account	List			
ListTagsForResource	Grants permission to list tags for a resource	Read			
StartCapacityTask	Grants permission to create a capacity task	Write	outpost*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartConnection	Grants permission to start a connection for your Outpost server	Write			
TagResource	Grants permission to tag a resource	Tagging	outpost		
			site		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	outpost		
			site		
				aws:TagKeys	
UpdateOutpost	Grants permission to update an Outpost	Write	outpost*		
UpdateSite	Grants permission to update a site	Write	site*		
UpdateSiteAddress	Grants permission to update the site address	Write	site*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSiteRackPhysicalProperties	Grants permission to update the physical properties of a rack at a site	Write	site*		

Resource types defined by AWS Outposts

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
outpost	`arn:${Partition}:outposts:${Region}:${Account}:outpost/${OutpostId}`	aws:ResourceTag/${TagKey}
site	`arn:${Partition}:outposts:${Region}:${Account}:site/${SiteId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Outposts

AWS Outposts defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Panorama

AWS Panorama (service prefix: `panorama`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Panorama
- Resource types defined by AWS Panorama
- Condition keys for AWS Panorama

Actions defined by AWS Panorama

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplicationInstance	Grants permission to create an AWS Panorama Application Instance	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateJobForDevices	Grants permission to create a job for an AWS Panorama Appliance	Write			
CreateNodeFromTemplateJob	Grants permission to create an AWS Panorama Node	Write			
CreatePackage	Grants permission to create an AWS Panorama Package	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePackageImportJob	Grants permission to create an AWS Panorama Package	Write			
DeleteDevice	Grants permission to deregister an AWS Panorama Appliance	Write	device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePackage	Grants permission to delete an AWS Panorama Package	Write	package*		
DeregisterPackageVersion	Grants permission to deregister an AWS Panorama package version	Write	package*		
DescribeApplicationInstance	Grants permission to view details about an AWS Panorama application instance	Read	applicationInstance*		
DescribeApplicationInstanceDetails	Grants permission to view details about an AWS Panorama application instance	Read	applicationInstance*		
DescribeDevice	Grants permission to view details about an AWS Panorama Appliance	Read	device*		
DescribeDeviceJob	Grants permission to view job details for an AWS Panorama Appliance	Read			
DescribeNode	Grants permission to view details about an AWS Panorama application node	Read			
DescribeNodeFromTemplateJob	Grants permission to view details about AWS Panorama application node	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePackage	Grants permission to view details about an AWS Panorama package	Read	package*		
DescribePackageImportJob	Grants permission to view details about an AWS Panorama package	Read			
DescribePackageVersion	Grants permission to view details about an AWS Panorama package version	Read	package*		
DescribeSoftware [permission only]	Grants permission to view details about a software version for the AWS Panorama Appliance	Read			
GetWebSocketURL [permission only]	Grants permission to generate a WebSocket endpoint for communication with AWS Panorama	Read			
ListApplicationInstanceDependencies	Grants permission to retrieve a list of application instance dependencies in AWS Panorama	List	applicationInstance*		
ListApplicationInstanceNodeInstances	Grants permission to retrieve a list of node instances of application instances in AWS Panorama	List	applicationInstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplicationInstances	Grants permission to retrieve a list of application instances in AWS Panorama	List	device		
ListDevices	Grants permission to retrieve a list of appliances in AWS Panorama	List			
ListDevicesJobs	Grants permission to retrieve a list of jobs for an AWS Panorama Appliance	List	device		
ListNodeFromTemplateJobs	Grants permission to retrieve a list of Nodes for an AWS Panorama Appliance	List			
ListNodes	Grants permission to retrieve a list of nodes in AWS Panorama	List			
ListPackageImportJobs	Grants permission to retrieve a list of packages in AWS Panorama	List			
ListPackages	Grants permission to retrieve a list of packages in AWS Panorama	List			
ListTagsForResource	Grants permission to retrieve a list of tags for a resource in AWS Panorama	Read	applicationInstance		
			device		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			package		
ProvisionDevice	Grants permission to register an AWS Panorama Appliance	Write		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterPackageVersion	Grants permission to register an AWS Panorama package version	Write	package*		
RemoveApplicationInstance	Grants permission to remove an AWS Panorama application instance	Write	applicationInstance*		
SignalApplicationInstanceNodeInstances	Grants permission to signal camera nodes in an application instance to pause or resume	Write	applicationInstance*		
TagResource	Grants permission to add tags to a resource in AWS Panorama	Tagging	applicationInstance		
			device		
			package		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource in AWS Panorama	Tagging	applicationInstance		
			device		
			package		
				aws:TagKeys	
UpdateDeviceMetadata	Grants permission to modify basic settings for an AWS Panorama Appliance	Write	device*		

Resource types defined by AWS Panorama

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:${Partition}:panorama:${Region}:${Account}:device/${DeviceId}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:panorama:${Region}:${Account}:package/${PackageId}	aws:ResourceTag/${TagKey}
applicationInstance	arn:${Partition}:panorama:${Region}:${Account}:applicationInstance/${ApplicationInstanceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Panorama

AWS Panorama defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Parallel Computing Service

AWS Parallel Computing Service (service prefix: `pcs`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Parallel Computing Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for AWS PCS cluster logs	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create clusters	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:CreateSecret secretsmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateComputeNodeGroup	Grants permission to create compute node groups	Write	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateQueue	Grants permission to create queues	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCluster	Grants permission to delete clusters	Write	cluster*		ec2:DeleteNetworkInterface secretsmanager:DeleteSecret
DeleteComputeNodeGroup	Grants permission to delete compute node groups	Write	cluster*		ec2:DeleteLaunchTemplate ec2:TerminateInstances
			computenodegroup*		
DeleteQueue	Grants permission to delete queues	Write	cluster*		
			queue*		
GetCluster	Grants permission to get cluster properties	Read	cluster*		
GetComputeNodeGroup	Grants permission to get compute node group properties	Read	cluster*		
			computenodegroup*		
GetQueue	Grants permission to get queue properties	Read	cluster*		
			queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClusters	Grants permission to list clusters	List			
ListComputeNodeGroups	Grants permission to list compute node groups	List	cluster*		
ListQueues	Grants permission to list queues	List	cluster*		
ListTagsForResource	Grants permission to list the tags for a resource	Read			
RegisterComputeNodeGroupInstance	Grants permission to register a compute instance in a compute node group	Write	cluster*		secretsmanager:GetSecretValue
TagResource	Grants permission to tag a resource	Tagging	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	cluster	aws:ResourceTag/${TagKey}	
			computenodegroup	aws:ResourceTag/${TagKey}	
			queue	aws:ResourceTag/${TagKey}	
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	Grants permission to update cluster properties	Write	cluster*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:CreateSecret secretsmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateComputeNodeGroup	Grants permission to update compute node group properties	Write	cluster*		ec2:CreateFleet ec2:CreateLaunchTemplate ec2:CreateLaunchTemplateVersion ec2:CreateTags ec2:DescribeImages ec2:DescribeInstanceStatus ec2:DescribeInstanceTypes ec2:DescribeInstances ec2:DescribeLaunchTemplateVersions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeLaunchTemplates ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:RunInstances iam:GetInstanceProfile iam:PassRole
			computenodegroup*		
UpdateQueue	Grants permission to update queue properties	Write	cluster*		
			queue*		

Resource types defined by AWS Parallel Computing 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:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}`	aws:ResourceTag/${TagKey}
computenodegroup	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/computenodegroup/${ComputeNodeGroupIdentifier}`	aws:ResourceTag/${TagKey}
queue	`arn:${Partition}:pcs:${Region}:${Account}:cluster/${ClusterIdentifier}/queue/${QueueIdentifier}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Parallel Computing Service

AWS Parallel Computing Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

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 AWS Partner Central

AWS Partner Central (service prefix: `partnercentral`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Partner Central
- Resource types defined by AWS Partner Central
- Condition keys for AWS Partner Central

Actions defined by AWS Partner Central

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptChannelHandshake	Grants permission to accept channel handshakes in AWS Partner Central	Write	ChannelHandshake*		
				partnercentral:Catalog partnercentral:ChannelHandshakeType	
AcceptConnectionInvitation	Grants permission to accept connection invitations in AWS Partner Central	Write	ConnectionInvitation*		
				partnercentral:Catalog	
AcceptEngagementInvitation	Grants permission to accept Engagement Invitations on AWS Partner Central	Write	engagement-invitation*		
				partnercentral:Catalog	
AmendBenefitApplication	Grants permission to amend benefit applications in AWS Partner Central	Write	BenefitApplication*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
AssignOpportunity	Grants permission to assign Opportunities on AWS Partner Central	Write	Opportunity*		
				partnercentral:Catalog	
AssociateAwsTrainingCertificationEmailDomain	Grants permission to associate AWS Training and Certification email domains in AWS Partner Central	Write	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate BenefitApplication Resource	Grants permission to associate benefit application resources in AWS Partner Central	Write	BenefitAllocation*		
			BenefitApplication*		
			Opportunity*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
Associate Opportunity	Grants permission to associate Opportunities on AWS Partner Central with other entities	Write	Opportunity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				partnercentral:Catalog partnercentral:RelatedEntityType	
CancelBenefitApplication	Grants permission to cancel benefit applications in AWS Partner Central	Write	BenefitApplication*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
CancelChannelHandshake	Grants permission to cancel channel handshakes in AWS Partner Central	Write	ChannelHandshake*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:ChannelHandshakeType	
CancelConnection	Grants permission to cancel connections in AWS Partner Central	Write	Connection*		
				partnercentral:Catalog	
CancelConnectionInvitation	Grants permission to cancel connection invitations in AWS Partner Central	Write	ConnectionInvitation*		
				partnercentral:Catalog	
CancelProfileUpdateTask	Grants permission to cancel profile update tasks in AWS Partner Central	Write	Partner*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBenefitApplication	Grants permission to create benefit applications in AWS Partner Central	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
CreateBusinessPlan [permission only]	Grants permission to create business plans in AWS Partner Central	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateChannelHandshake	Grants permission to create channel handshakes in AWS Partner Central	Write	ProgramManagementAccount		
			Relationship		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:ChannelHandshakeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCollaborationChannelMembers [permission only]	Grants permission to create collaboration channel members in AWS Partner Central	Write			
CreateCollaborationChannelRequest [permission only]	Grants permission to create collaboration channel requests in AWS Partner Central	Write			
CreateConnectionInvitation	Grants permission to create connection invitations in AWS Partner Central	Write		partnercentral:Catalog	
CreateEngagement	Grants permission to creating engagements in AWS Partner Central	Write	Engagement*		
				partnercentral:Catalog	
CreateEngagementContext	Grants permission to create engagement contexts in AWS Partner Central	Write	Engagement*		
				partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEngagementInvitation	Grants permission to creating engagement invitations in AWS Partner Central	Write	engagement-invitation*		
				partnercentral:Catalog	
CreateOpportunity	Grants permission to create new Opportunities on AWS Partner Central	Write	Opportunity*		
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePartner	Grants permission to create partners in AWS Partner Central	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
CreateProgramManagementAccount	Grants permission to create program management accounts in AWS Partner Central	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRelationship	Grants permission to create relationships in AWS Partner Central	Write	ProgramManagementAccount*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
CreateResourceSnapshot	Grants permission to creating resource snapshots in AWS Partner Central	Write	ResourceSnapshot*		
				partnercentral:Catalog	
CreateResourceSnapshotJob	Grants permission to creating resource snapshot jobs in AWS Partner Central	Write	resource-snapshot-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys partnercentral:Catalog	
DeleteProgramManagementAccount	Grants permission to delete program management accounts in AWS Partner Central	Write	ProgramManagementAccount*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
DeleteRelationship	Grants permission to delete relationships in AWS Partner Central	Write	Relationship*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
DeleteResourceSnapshotJob	Grants permission to deleting resource snapshot jobs on AWS Partner Central	Write	resource-snapshot-job*		
				partnercentral:Catalog	
DisassociateAwsTrainingCertificationEmailDomain	Grants permission to disassociate AWS Training and Certification email domains in AWS Partner Central	Write	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
DisassociateBenefitApplicationResource	Grants permission to disassociate benefit application resources in AWS Partner Central	Write	BenefitAllocation*		
			BenefitApplication*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Opportunity*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
DisassociateOpportunity	Grants permission to disassociate Opportunities on AWS Partner Central from other entities	Write	Opportunity*		
				partnercentral:Catalog partnercentral:RelatedEntityType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnrollInPartnerPath [permission only]	Grants permission to enroll in partner paths in AWS Partner Central	Write			
GetAllianceLeadContact	Grants permission to retrieve alliance lead contact information in AWS Partner Central	Read	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetAwsOpportunitySummary	Grants permission to retrieve AWS Opportunity Summaries for Opportunities on AWS Partner Central	Read	Opportunity*		
				partnercentral:Catalog	
GetBenefit	Grants permission to retrieve benefit details in AWS Partner Central	Read	Benefit*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
GetBenefitAllocation	Grants permission to retrieve benefit allocation details in AWS Partner Central	Read	BenefitAllocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes	
GetBenefitApplication	Grants permission to retrieve benefit application details in AWS Partner Central	Read	BenefitApplication*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
GetBusinessPlan [permission only]	Grants permission to retrieve business plan details in AWS Partner Central	Read			
GetCollaborationChannel [permission only]	Grants permission to retrieve collaboration channel details in AWS Partner Central	Read			
GetConnection	Grants permission to retrieve connection details in AWS Partner Central	Read	Connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				partnercentral:Catalog	
GetConnectionInvitation	Grants permission to retrieve connection invitation details in AWS Partner Central	Read	ConnectionInvitation*		
				partnercentral:Catalog	
GetConnectionPreferences	Grants permission to retrieve connection preferences in AWS Partner Central	Read		partnercentral:Catalog	
GetEngagement	Grants permission to retrieval of engagement details in AWS Partner Central	Read	Engagement*		
				partnercentral:Catalog	
GetEngagementInvitation	Grants permission to retrieve details of Engagement Invitations on AWS Partner Central	Read	engagement-invitation*		
				partnercentral:Catalog	
GetOpportunity	Grants permission to retrieve details of Opportunities on AWS Partner Central	Read	Opportunity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				partnercentral:Catalog	
GetPartner	Grants permission to retrieve partner details in AWS Partner Central	Read	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetPartnerDashboard	Grants permission to retrieve partner dashboard information in AWS Partner Central	Read	Dashboard*		
				partnercentral:Catalog	
GetPartnerProfile [permission only]	Grants permission to retrieve public partner profile details in AWS Partner Central	Read			
GetProfileUpdateTask	Grants permission to retrieve profile update task details in AWS Partner Central	Read	Partner*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetProfileVisibility	Grants permission to retrieve profile visibility settings in AWS Partner Central	Read	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetProgramManagementAccount [permission only]	Grants permission to retrieve program management account details in AWS Partner Central	Read		partnercentral:Catalog	
GetRelationship	Grants permission to retrieve relationship details in AWS Partner Central	Read	Relationship*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
GetResourceSnapshot	Grants permission to retrieving resource snapshot details in AWS Partner Central	Read	ResourceSnapshot*		
				partnercentral:Catalog	
GetResourceSnapshotJob	Grants permission to retrieving resource snapshot job details in AWS Partner Central	Read	resource-snapshot-job*		
				partnercentral:Catalog	
GetSellingSystemSettings	Grants permission to retrieving selling system settings in AWS Partner Central	Read		partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerification	Grants permission to retrieve verification details in AWS Partner Central	Read		partnercentral:Catalog partnercentral:VerificationType	
ListBenefitAllocations	Grants permission to list benefit allocations in AWS Partner Central	List	BenefitAllocation*		
				partnercentral:Catalog partnercentral:FulfillmentTypes	
ListBenefitApplications	Grants permission to list benefit applications in AWS Partner Central	List	BenefitApplication*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
ListBenefits	Grants permission to list benefits in AWS Partner Central	List	Benefit*		
				partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
ListBusinessPlans [permission only]	Grants permission to list business plans in AWS Partner Central	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChannelHandshakes	Grants permission to list channel handshakes in AWS Partner Central	List	ChannelHandshake*		
				partnercentral:Catalog partnercentral:ChannelHandshakeType	
ListCollaborationChannels [permission only]	Grants permission to list collaboration channels in AWS Partner Central	List			
ListConnectionInvitations	Grants permission to list connection invitations in AWS Partner Central	List		partnercentral:Catalog	
ListConnections	Grants permission to list connections in AWS Partner Central	List		partnercentral:Catalog	
ListEngagementByAcceptingInvitationTasks	Grants permission to listing engagements by accepting invitation tasks in AWS Partner Central	List		partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEngagementFromOpportunityTasks	Grants permission to listing engagements from opportunity tasks in AWS Partner Central	List		partnercentral:Catalog	
ListEngagementInvitations	Grants permission to list Engagement Invitations on AWS Partner Central	List		partnercentral:Catalog	
ListEngagementMembers	Grants permission to listing engagement members in AWS Partner Central	Read	Engagement*		
				partnercentral:Catalog	
ListEngagementResourceAssociations	Grants permission to listing engagement resource associations in AWS Partner Central	Read	ResourceSnapshot*		
				partnercentral:Catalog	
ListEngagements	Grants permission to listing engagements in AWS Partner Central	List		partnercentral:Catalog	
ListOpportunities	Grants permission to list Opportunities on AWS Partner Central	List		partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOpportunityFromEngagementTasks	Grants permission to list opportunity from engagement tasks in AWS Partner Central	List		partnercentral:Catalog	
ListPartnerPaths [permission only]	Grants permission to list partner paths in AWS Partner Central	List			
ListPartners	Grants permission to list partners in AWS Partner Central	List		partnercentral:Catalog	
ListProgramManagementAccounts	Grants permission to list program management accounts in AWS Partner Central	List	ProgramManagementAccount*		
				partnercentral:Catalog	
ListRelationships	Grants permission to list relationships in AWS Partner Central	List	Relationship*		
				partnercentral:Catalog	
ListResourceSnapshotJobs	Grants permission to listing resource snapshot jobs in AWS Partner Central	List		partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceSnapshots	Grants permission to listing resource snapshots in AWS Partner Central	List	ResourceSnapshot*		
				partnercentral:Catalog	
ListSolutions	Grants permission to list Solutions on AWS Partner Central	List		partnercentral:Catalog	
ListTagsForResource	Grants permission to add lists tags to a resource. Supported resource: ResourceSnapshotJob	Read		aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAllianceLeadContact	Grants permission to set alliance lead contact information in AWS Partner Central	Write	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
PutBusinessPlan [permission only]	Grants permission to update business plans in AWS Partner Central	Write			
PutProfileVisibility	Grants permission to set profile visibility in AWS Partner Central	Write	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
PutSellingSystemSettings	Grants permission to put selling system settings in AWS Partner Central	Write			
RecallBenefitApplication	Grants permission to recall benefit applications in AWS Partner Central	Write	BenefitApplication*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
RejectChannelHandshake	Grants permission to reject channel handshakes in AWS Partner Central	Write	ChannelHandshake*		
				partnercentral:Catalog partnercentral:ChannelHandshakeType	
RejectConnectionInvitation	Grants permission to reject connection invitations in AWS Partner Central	Write	ConnectionInvitation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				partnercentral:Catalog	
RejectEngagementInvitation	Grants permission to reject Engagement Invitations on AWS Partner Central	Write	engagement-invitation*		
				partnercentral:Catalog	
SearchPartnerProfiles [permission only]	Grants permission to search public partner profiles in AWS Partner Central	List			
SendEmailVerificationCode	Grants permission to send email verification codes in AWS Partner Central	Write		partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartEngagementByAcceptingInvitationTask	Grants permission to initiate tasks that start Engagements on AWS Partner Central by accepting an Engagement Invitation	Write	engagement-by-accepting-invitation-task*		partnercentral:AcceptEngagementInvitation partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagementInvitation partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartEngagementFromOpportunityTask	Grants permission to initiate tasks that start Engagements from Opportunities on AWS Partner Central	Write	engagement-from-opportunity-task*		partnercentral:CreateEngagement partnercentral:CreateEngagementInvitation partnercentral:CreateResourceSnapshotJob partnercentral:GetOpportunity partnercentral:StartResourceSnapshotJob partnercentral:SubmitOpportunity

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartOpportunityFromEngagementTask	Grants permission to initiate tasks that start Opportunities from Engagements on AWS Partner Central	Write	OpportunityFromEngagementTask*		partnercentral:CreateEngagementContext partnercentral:CreateOpportunity partnercentral:CreateResourceSnapshot partnercentral:CreateResourceSnapshotJob partnercentral:GetEngagement partnercentral:StartResourceSnapshotJob

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog	
StartProfileUpdateTask	Grants permission to start profile update tasks in AWS Partner Central	Write	Partner*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
StartResourceSnapshotJob	Grants permission to starting resource snapshot jobs in AWS Partner Central	Write	resource-snapshot-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				partnercentral:Catalog	
StartVerification	Grants permission to start verification processes in AWS Partner Central	Write		partnercentral:Catalog partnercentral:VerificationType	
StopResourceSnapshotJob	Grants permission to stopping resource snapshot jobs in AWS Partner Central	Write	resource-snapshot-job*		
				partnercentral:Catalog	
SubmitBenefitApplication	Grants permission to submit benefit applications in AWS Partner Central	Write	BenefitApplication*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
SubmitOpportunity	Grants permission to submit Opportunities on AWS Partner Central	Write	Opportunity*		
				partnercentral:Catalog	
TagResource	Grants permission to add new tags to a resource. Supported resource: ResourceSnapshotJob	Tagging	BenefitApplication		
			ChannelHandshake		
			Opportunity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Partner		
			ProgramManagementAccount		
			Relationship		
			resource-snapshot-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
UntagResource	Grants permission to remove tags from a resource. Supported resource: ResourceSnapshotJob	Tagging	BenefitApplication		
			ChannelHandshake		
			Opportunity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Partner		
			ProgramManagementAccount		
			Relationship		
			resource-snapshot-job		
				aws:ResourceTag/${TagKey} aws:TagKeys partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBenefitApplication	Grants permission to update benefit applications in AWS Partner Central	Write	BenefitApplication*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog partnercentral:FulfillmentTypes partnercentral:Programs	
UpdateConnectionPreferences	Grants permission to update connection preferences in AWS Partner Central	Write		partnercentral:Catalog	
UpdateEngagementContext	Grants permission to update engagement contexts in AWS Partner Central	Write	Engagement*		
				partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOpportunity	Grants permission to update Opportunities on AWS Partner Central	Write	Opportunity*		
				partnercentral:Catalog	
UpdateProgramManagementAccount	Grants permission to update program management accounts in AWS Partner Central	Write	ProgramManagementAccount*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	
UpdateRelationship	Grants permission to update relationships in AWS Partner Central	Write	Relationship*		
				aws:ResourceTag/${TagKey} partnercentral:Catalog	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UseSession [permission only]	Grants permission to use Partner Central Agents sessions in AWS Partner Central	Write		partnercentral:Catalog	

Resource types defined by AWS Partner Central

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
Engagement	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement/${Identifier}`	
engagement-by-accepting-invitation-task	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-by-accepting-invitation-task/${TaskId}`	
engagement-from-opportunity-task	`arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-from-opportunity-task/${TaskId}`	

Resource types	ARN	Condition keys
engagement-invitation	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/engagement-invitation/${Identifier}	
Opportunity	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/opportunity/${Identifier}	aws:ResourceTag/${TagKey}
resource-snapshot-job	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/resource-snapshot-job/${Identifier}	aws:ResourceTag/${TagKey}
ResourceSnapshot	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/engagement/${EngagementIdentifier}/resource/${ResourceType}/${ResourceIdentifier}/template/${TemplateIdentifier}/resource-snapshot/${SnapshotRevision}	
Solution	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/solution/${Identifier}	
Partner	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/partner/${Identifier}	aws:ResourceTag/${TagKey}
Connection	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/connection/${Identifier}	
ConnectionInvitation	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/connection-invitation/${Identifier}	

Resource types	ARN	Condition keys
ConnectionPreferences	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/connection-preferences	
OpportunityFromEngagementTask	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/opportunity-from-engagement-task/${TaskId}	
Benefit	arn:${Partition}:partnercentral:${Region}::catalog/${Catalog}/benefit/${Identifier}	
BenefitAllocation	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/benefit-allocation/${Identifier}	
BenefitApplication	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/benefit-application/${Identifier}	aws:ResourceTag/${TagKey}
ProgramManagementAccount	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/program-management-account/${Identifier}	aws:ResourceTag/${TagKey}
Relationship	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/program-management-account/${ProgramManagementAccountId}/relationship/${RelationshipId}	aws:ResourceTag/${TagKey}
ChannelHandshake	arn:${Partition}:partnercentral:${Region}:${Account}:catalog/${Catalog}/channel-handshake/${Identifier}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Dashboard	arn:${Partition}:partnercentral::${Account}:catalog/${Catalog}/ReportingData/${TableId}/Dashboard/${DashboardId}	

Condition keys for AWS Partner Central

AWS Partner Central defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
partnercentral:Catalog	Filters access by a specific Catalog	String
partnercentral:ChannelHandshakeType	Filters access by channel handshake types	String

Condition keys	Description	Type
partnercentral:FulfillmentTypes	Filters access by benefit fulfillment types	ArrayOfString
partnercentral:Programs	Filters access by program	ArrayOfString
partnercentral:RelatedEntityType	Filters access by entity types for Opportunity association	String
partnercentral:VerificationType	Filters access by the type of verification being performed	String

Actions, resources, and condition keys for AWS Partner central account management

AWS Partner central account management (service prefix: `partnercentral-account-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 AWS Partner central account management
- Resource types defined by AWS Partner central account management
- Condition keys for AWS Partner central account management

Actions defined by AWS Partner central account management

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessLegacyPartnerCentral [permission only]	Grants permission to Single Sign-On from AWS Partner Central into Legacy Partner Central	Write		partnercentral-account-management:LegacyPartnerCentralRole	
AccessMarketingCentral [permission only]	Grants permission to Single Sign-On from AWS Partner Central into Marketing Central	Write		partnercentral-account-management:MarketingCentralRole	
AccessProServeTools [permission only]	Grants permission to Single Sign-On from AWS Partner Central into ProServe Tools	Write		partnercentral-account-management:ProServeRole	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociatePartnerAccount [permission only]	Grants permission to associate Partner account to AWS account	Write			
AssociatePartnerUser	Grants permission to associate Partner user to IAM role	Write			
DisassociatePartnerUser	Grants permission to disassociate Partner user to IAM role	Write			

Resource types defined by AWS Partner central account management

AWS Partner central account management does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Partner central account management, specify `"Resource": "*"` in your policy.

Condition keys for AWS Partner central account management

AWS Partner central account management defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
partnercentral-account-management:LegacyPartnerCentralRole	Filters access by the Legacy Partner Central role	ArrayOfString
partnercentral-account-management:MarketingCentralRole	Filters access by Marketing Central role	ArrayOfString
partnercentral-account-management:ProServeRole	Filters access by ProServe Tools role	ArrayOfString

Actions, resources, and condition keys for AWS Payment Cryptography

AWS Payment Cryptography (service prefix: `payment-cryptography`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Payment Cryptography
- Resource types defined by AWS Payment Cryptography
- Condition keys for AWS Payment Cryptography

Actions defined by AWS Payment Cryptography

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddKeyReplicationRegions	Grants permission to add replication regions to an existing AWS Payment Cryptography key	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
CreateAlias	Grants permission to create a user-friendly name for a Key	Write	alias*		
			key*		
CreateKey	Grants permission to create a unique customer managed key in the caller's AWS account and region	Write		aws:RequestTag/${TagKey} aws:TagKeys payment-cryptography:KeyClass	payment-cryptography:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				payment-cryptography:KeyUsage payment-cryptography:KeyAlgorithm	
DecryptData	Grants permission to decrypt ciphertext data to plaintext using symmetric, asymmetric or DUKPT data encryption key	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
DeleteAlias	Grants permission to delete the specified alias	Write	alias*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteKey	Grants permission to schedule the deletion of a Key	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				payment-cryptography:RequestAlias	
DisableDefaultKeyReplicationRegions	Grants permission to disable default key replication regions for account-level replication	Write			
EnableDefaultKeyReplicationRegions	Grants permission to enable default key replication regions for account-level replication	Write			
EncryptData	Grants permission to encrypt plaintext data to ciphertext using symmetric, asymmetric or DUKPT data encryption key	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
ExportKey	Grants permission to export a key from the service	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				payment-cryptography:RequestAlias payment-cryptography:CertificateAuthorityPublicKeyIdentifier payment-cryptography:WrappingKeyIdentifier	
GenerateAs2805KekValidation	Grants permission to generate a KekValidationRequest or a KekValidationResponse for node-to-node initialization between payment processing nodes using Australian Standard 2805 (AS2805)	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateCardValidationData	Grants permission to generate card-related data using algorithms such as Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) or Card Security Codes (CSC) that check the validity of a magnetic stripe card	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
GenerateMac	Grants permission to generate a MAC (Message Authentication Code) cryptogram	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
GenerateMacEmvPinChange	Grants permission to generate a MAC (Message Authentication Code) cryptogram	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GeneratePinData	Grants permission to generate pin-related data such as PIN, PIN Verification Value (PVV), PIN Block and PIN Offset during new card issuance or card re-issuance	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
GetAlias	Grants permission to return the keyArn associated with an aliasName	Read	alias*		
			key*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCertificateSigningRequest	Grants permission to return the Certificate Signing Request for a public key from a key of class PUBLIC_KEY	Read	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDefaultKeyReplicationRegions	Grants permission to retrieve the default key replication regions configured at the account level	Read			
GetKey	Grants permission to return the detailed information about the specified key	Read	key*		
				payment-cryptography:RequestAlias	
GetParametersForExport	Grants permission to get the export token and the signing key certificate to initiate a TR-34 key export	Read			
GetParametersForImport	Grants permission to get the import token and the wrapping key certificate to initiate a TR-34 key import	Read			
GetPublicKeyCertificate	Grants permission to return the public key from a key of class PUBLIC_KEY	Read	key*		
				payment-cryptography:RequestAlias	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportKey	Grants permission to imports keys and public key certificates	Write		aws:RequestTag/${TagKey} aws:TagKeys payment-cryptography:ImportKeyMaterial payment-cryptography:CertificateAuthorityPublicKeyIdentifier payment-cryptography:WrappingKeyIdentifier	payment-cryptography:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAliases	Grants permission to return a list of aliases created for all keys in the caller's AWS account and Region	List			
ListKeys	Grants permission to return a list of keys created in the caller's AWS account and Region	List			
ListTagsForResource	Grants permission to return a list of tags created in the caller's AWS account and Region	Read	key		
ReEncryptData	Grants permission to re-encrypt ciphertext using DUKPT, Symmetric and Asymmetric Data Encryption Keys	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
RemoveKeyReplicationRegions	Grants permission to remove replication regions from an existing AWS Payment Cryptography key	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreKey	Grants permission to cancel a scheduled key deletion if at any point during the waiting period a Key needs to be revived	Write	key*		
				payment-cryptography:RequestAlias	
StartKeyUsage	Grants permission to enable a disabled Key	Write	key*		
				payment-cryptography:RequestAlias	
StopKeyUsage	Grants permission to disable an enabled Key	Write	key*		
				payment-cryptography:RequestAlias	
TagResource	Grants permission to add or overwrites one or more tags for the specified resource	Tagging	key*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TranslateKeyMaterial	Grants permission to translate wrapping key type for a wrapped key	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
TranslatePinData	Grants permission to translate encrypted PIN block from and to ISO 9564 formats 0,1,3,4	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
UntagResource	Grants permission to remove the specified tag or tags from the specified resource	Tagging	key*		
				aws:TagKeys	
UpdateAlias	Grants permission to change the key to which an alias is assigned, or unassign it from its current key	Write	alias*		
			key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyAuthRequestCryptogram	Grants permission to verify Authorization Request Cryptogram (ARQC) for a EMV chip payment card authorization	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
VerifyCardValidationData	Grants permission to verify card-related validation data using algorithms such as Card Verification Values (CVV/CVV2), Dynamic Card Verification Values (dCVV/dCVV2) and Card Security Codes (CSC)	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	
VerifyMac	Grants permission to verify MAC (Message Authentication Code) of input data against a provided MAC	Write	alias*		
			key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				payment-cryptography:RequestAlias	
VerifyPinData	Grants permission to verify pin-related data such as PIN and PIN Offset using algorithms including VISA PVV and IBM3624	Write	alias*		
			key*		
				payment-cryptography:RequestAlias	

Resource types defined by AWS Payment Cryptography

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
key	`arn:${Partition}:payment-cryptography:${Region}:${Account}:key/${KeyId}`	aws:ResourceTag/${TagKey} payment-cryptography:ResourceAliases

Resource types	ARN	Condition keys
alias	arn:${Partition}:payment-cryptography:${Region}:${Account}:alias/${Alias}	payment-cryptography:ResourceAliases

Condition keys for AWS Payment Cryptography

AWS Payment Cryptography defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by both the key and value of the tag in the request for the specified operation	String
aws:ResourceTag/${TagKey}	Filters access by tags assigned to a key for the specified operation	String
aws:TagKeys	Filters access by the tag keys in the request for the specified operation	ArrayOfString
payment-cryptography:CertificateAuthorityPublicKeyIdentifier	Filters access by the CertificateAuthorityPublicKeyIdentifier specified in the request or the ImportKey, and ExportKey operations	String
payment-cryptograp	Filters access by the type of key material being imported [RootCertificatePublicKey, TrustedCertificatePublicKey	String

Condition keys	Description	Type
hy:Import KeyMaterial	, Tr34KeyBlock, Tr31KeyBlock, DiffieHellmanTr31K eyBlock, As2805KeyCryptogram] for the ImportKey operation	
payment-cryptograp hy:KeyAlgorithm	Filters access by KeyAlgorithm specified in the request for the CreateKey operation	String
payment-cryptograp hy:KeyClass	Filters access by KeyClass specified in the request for the CreateKey operation	String
payment-cryptograp hy:KeyUsage	Filters access by KeyClass specified in the request or associated with a key for the CreateKey operation	String
payment-cryptograp hy:RequestAlias	Filters access by aliases in the request for the specified operation	String
payment-cryptograp hy:Resour ceAliases	Filters access by aliases associated with a key for the specified operation	ArrayOfString
payment-cryptograp hy:Wrappi ngKeyIdentifier	Filters access by the WrappingKeyIdentifier specified in the request for the ImportKey, and ExportKey operation s	String

Actions, resources, and condition keys for AWS Payments

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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 AWS Payments

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Performance Insights

AWS Performance Insights (service prefix: `pi`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Performance Insights
- Resource types defined by AWS Performance Insights
- Condition keys for AWS Performance Insights

Actions defined by AWS Performance Insights

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePerformanceAnalysisReport	Grants permission to call CreatePerformanceAnalysisReport API to create a Performance Analysis Report for a specified DB instance	Write	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePerformanceAnalysisReport	Grants permission to call DeletePerformanceAnalysisReport API to delete a Performance Analysis Report for a specified DB instance	Write	perf-reports-resource*		
DescribeDimensionKeys	Grants permission to call DescribeDimensionKeys API to retrieve the top N dimension keys for a metric for a specific time period	Read	metric-resource*		
				pi:Dimensions	
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	Read	perf-reports-resource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Performance Analysis Report for a specified DB instance				
GetResourceMetadata	Grants permission to call GetResourceMetadata API to retrieve the metadata for different features	Read	metric-resource*		
GetResourceMetrics	Grants permission to call GetResourceMetrics API to retrieve PI metrics for a set of data sources, over a time period	Read	metric-resource*		
				pi:Dimensions	
ListAvailableResourceDimensions	Grants permission to call ListAvailableResourceDimensions API to retrieve the dimensions that can be queried for each specified metric type on a specified DB instance	Read	metric-resource*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPerformanceAnalysisReports	Grants permission to call ListPerformanceAnalysisReports API to list Performance Analysis Reports for a specified DB instance	List	perf-reports-resource*		
ListTagsForResource	Grants permission to call ListTagsForResource API to list tags for a resource	List	metric-resource*		
			perf-reports-resource*		
TagResource	Grants permission to call TagResource API to tag a resource	Tagging	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to call UntagResource API to untag a resource	Tagging	perf-reports-resource*		
				aws:TagKeys	

Resource types defined by AWS Performance Insights

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	aws:ResourceTag/${TagKey}
perf-reports-resource	`arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Performance Insights

AWS Performance Insights defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListEventTrackers	Grants permission to list event trackers	List			
ListFilters	Grants permission to list filters	List			
ListMetricAttributionMetrics	Grants permission to list metric attribution metrics	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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}`	
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}`	

Resource types	ARN	Condition keys
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}	
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}	

Resource types	ARN	Condition keys
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 AWS global condition context keys.

Actions, resources, and condition keys for Amazon Pinpoint

Amazon Pinpoint (service prefix: mobiletargeting) 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 Pinpoint
- Resource types defined by Amazon Pinpoint
- Condition keys for Amazon Pinpoint

Actions defined by Amazon Pinpoint

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApp	Grants permission to create an app	Write	apps*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateCampaign	Grants permission to create a campaign for an app	Write	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateEmailTemplate	Grants permission to create an email template	Write	template*		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateExportJob	Grants permission to create an export job that exports endpoint definitions to Amazon S3	Write	app*		
CreateImportJob	Grants permission to import endpoint definitions from to create a segment	Write	app*		
CreateInAppTemplate	Grants permission to create an in-app message template	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateJourney	Grants permission to create a Journey for an app	Write	journeys*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreatePushTemplate	Grants permission to create a push notification template	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateRecommenderConfiguration	Grants permission to create an Amazon Pinpoint configuration for a recommender model	Write	recommenders*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSegment	Grants permission to create a segment that is based on endpoint data reported to Pinpoint by your app. To allow a user to create a segment by importing endpoint data from outside of Pinpoint, allow the mobiletargeting:CreateImportJob action	Write	app*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateSmsTemplate	Grants permission to create an sms message template	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateVoiceTemplate	Grants permission to create a voice message template	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteAdmChannel	Grants permission to delete the ADM channel for an app	Write	channel*		
DeleteApnsChannel	Grants permission to delete the APNs channel for an app	Write	channel*		
DeleteApnsSandboxChannel	Grants permission to delete the APNs sandbox channel for an app	Write	channel*		
DeleteApnsVoipChannel	Grants permission to delete the APNs VoIP channel for an app	Write	channel*		
DeleteApnsVoipSandboxChannel	Grants permission to delete the APNs VoIP sandbox channel for an app	Write	channel*		
DeleteApp	Grants permission to delete a specific campaign	Write	app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBaiduChannel	Grants permission to delete the Baidu channel for an app	Write	channel*		
DeleteCampaign	Grants permission to delete a specific campaign	Write	campaign*		
DeleteEmailChannel	Grants permission to delete the email channel for an app	Write	channel*		
DeleteEmailTemplate	Grants permission to delete an email template or an email template version	Write	template*		
DeleteEndpoint	Grants permission to delete an endpoint	Write	endpoint*		
DeleteEventStream	Grants permission to delete the event stream for an app	Write	event-stream*		
DeleteGcmChannel	Grants permission to delete the GCM channel for an app	Write	channel*		
DeleteInAppTemplate	Grants permission to delete an in-app message template or an in-app message template version	Write	template*		
DeleteJourney	Grants permission to delete a specific journey	Write	journey*		
DeletePushTemplate	Grants permission to delete a push notification template or a push notification template version	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRecommenderConfiguration	Grants permission to delete an Amazon Pinpoint configuration for a recommender model	Write	recommender*		
DeleteSegment	Grants permission to delete a specific segment	Write	segment*		
DeleteSmsChannel	Grants permission to delete the SMS channel for an app	Write	channel*		
DeleteSmsTemplate	Grants permission to delete an sms message template or an sms message template version	Write	template*		
DeleteUserEndpoints	Grants permission to delete all of the endpoints that are associated with a user ID	Write	user*		
DeleteVoiceChannel	Grants permission to delete the Voice channel for an app	Write	channel*		
DeleteVoiceTemplate	Grants permission to delete a voice message template or a voice message template version	Write	template*		
GetAdmChannel	Grants permission to retrieve information about the Amazon Device Messaging (ADM) channel for an app	Read	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApnsChannel	Grants permission to retrieve information about the APNs channel for an app	Read	channel*		
GetApnsSandboxChannel	Grants permission to retrieve information about the APNs sandbox channel for an app	Read	channel*		
GetApnsVoipChannel	Grants permission to retrieve information about the APNs VoIP channel for an app	Read	channel*		
GetApnsVoipSandboxChannel	Grants permission to retrieve information about the APNs VoIP sandbox channel for an app	Read	channel*		
GetApp	Grants permission to retrieve information about a specific app in your Amazon Pinpoint account	Read	app*		
GetApplicationDateRangeKpi	Grants permission to retrieve (queries) pre-aggregated data for a standard metric that applies to an application	Read	application-metrics*		
GetApplicationSettings	Grants permission to retrieve the default settings for an app	List	app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApps	Grants permission to retrieve a list of apps in your Amazon Pinpoint account	Read	apps*		
GetBaiduChannel	Grants permission to retrieve information about the Baidu channel for an app	Read	channel*		
GetCampaign	Grants permission to retrieve information about a specific campaign	Read	campaign*		
GetCampaignActivities	Grants permission to retrieve information about the activities performed by a campaign	List	campaign*		
GetCampaignDateRangeKpi	Grants permission to retrieve (queries) pre-aggregated data for a standard metric that applies to a campaign	Read	campaign-metrics*		
GetCampaignVersion	Grants permission to retrieve information about a specific campaign version	Read	campaign*		
GetCampaignVersions	Grants permission to retrieve information about the current and prior versions of a campaign	List	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCampaigns	Grants permission to retrieve information about all campaigns for an app	List	app*		
GetChannels	Grants permission to get all channels information for your app	List	channels*		
GetEmailChannel	Grants permission to obtain information about the email channel in an app	Read	channel*		
GetEmailTemplate	Grants permission to retrieve information about a specific or the active version of an email template	Read	template*		
GetEndpoint	Grants permission to retrieve information about a specific endpoint	Read	endpoint*		
GetEventStream	Grants permission to retrieve information about the event stream for an app	Read	event-stream*		
GetExportJob	Grants permission to obtain information about a specific export job	Read	export-job*		
GetExportJobs	Grants permission to retrieve a list of all of the export jobs for an app	List	app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGcmChannel	Grants permission to retrieve information about the GCM channel for an app	Read	channel*		
GetImportJob	Grants permission to retrieve information about a specific import job	Read	import-job*		
GetImportJobs	Grants permission to retrieve information about all import jobs for an app	List	app*		
GetInAppMessages	Grants permission to retrive in-app messages for the given endpoint id	Read	app*		
GetInAppTemplate	Grants permission to retrieve information about a specific or the active version of an in-app message template	Read	template*		
GetJourney	Grants permission to retrieve information about a specific journey	Read	journey*		
GetJourneyDateRangeKpi	Grants permission to retrieve (queries) pre-aggregated data for a standard engagement metric that applies to a journey	Read	journey-metrics*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetJourneyExecutionActivityMetrics	Grants permission to retrieve (queries) pre-aggregated data for a standard execution metric that applies to a journey activity	Read	journey-execution-activity-metrics*		
GetJourneyExecutionMetrics	Grants permission to retrieve (queries) pre-aggregated data for a standard execution metric that applies to a journey	Read	journey-execution-metrics*		
GetJourneyRunExecutionActivityMetrics	Grants permission to retrieve (queries) pre-aggregated data for a standard execution metric that applies to a journey activity for a single journey run	Read	journey*		
GetJourneyRunExecutionMetrics	Grants permission to retrieve (queries) pre-aggregated data for a standard execution metric that applies to a journey for a single journey run	Read	journey*		
GetJourneyRuns	Grants permission to retrieve information about all journey runs for a journey	List	journey*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPushTemplate	Grants permission to retrieve information about a specific or the active version of an push notification template	Read	template*		
GetRecommenderConfiguration	Grants permission to retrieve information about an Amazon Pinpoint configuration for a recommender model	Read	recommender*		
GetRecommenderConfigurations	Grants permission to retrieve information about all the recommender model configurations that are associated with an Amazon Pinpoint account	List	recommenders*		
GetReports [permission only]	Grants permission to mobiletargeting:GetReports	Read	reports*		
GetSegment	Grants permission to retrieve information about a specific segment	Read	segment*		
GetSegmentExportJobs	Grants permission to retrieve information about jobs that export endpoint definitions from segments to Amazon S3	List	segment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSegmentImportJobs	Grants permission to retrieve information about jobs that create segments by importing endpoint definitions from	List	segment*		
GetSegmentVersion	Grants permission to retrieve information about a specific segment version	Read	segment*		
GetSegmentVersions	Grants permission to retrieve information about the current and prior versions of a segment	List	segment*		
GetSegments	Grants permission to retrieve information about the segments for an app	List	app*		
GetSmsChannel	Grants permission to obtain information about the SMS channel in an app	Read	channel*		
GetSmsTemplate	Grants permission to retrieve information about a specific or the active version of an sms message template	Read	template*		
GetUserEndpoints	Grants permission to retrieve information about the endpoints that are associated with a user ID	Read	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVoiceChannel	Grants permission to obtain information about the Voice channel in an app	Read	channel*		
GetVoiceTemplate	Grants permission to retrieve information about a specific or the active version of a voice message template	Read	template*		
ListJourneys	Grants permission to retrieve information about all journeys for an app	List	app*		
ListTagsForResource	Grants permission to list tags for a resource	Read	app		
			campaign		
			journey		
			segment		
			template		
ListTemplateVersions	Grants permission to retrieve all versions about a specific template	List	template*		
ListTemplates	Grants permission to retrieve metadata about the queried templates	List	templates*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PhoneNumberValidate	Grants permission to obtain metadata for a phone number, such as the number type (mobile, landline, or VoIP), location, and provider	Read	phone-number-validate*		
PutEventStream	Grants permission to create or update an event stream for an app	Write	event-stream*		
PutEvents	Grants permission to create or update events for an app	Write	events*		
RemoveAttributes	Grants permission to remove the attributes for an app	Write	attribute*		
SendMessages	Grants permission to send an SMS message or push notification to specific endpoints	Write	messages*		
SendOTPMessage	Grants permission to send an OTP code to a user of your application	Write	otp*		
SendUsersMessages	Grants permission to send an SMS message or push notification to all endpoints that are associated with a specific user ID	Write	messages*		
TagResource	Grants permission to add tags to a resource	Tagging	app campaign		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	app		
			campaign		
			journey		
			segment		
			template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateAdmChannel	Grants permission to update the Amazon Device Messaging (ADM) channel for an app	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApnsChannel	Grants permission to update the Apple Push Notification service (APNs) channel for an app	Write	channel*		
UpdateApnsSandboxChannel	Grants permission to update the Apple Push Notification service (APNs) sandbox channel for an app	Write	channel*		
UpdateApnsVoipChannel	Grants permission to update the Apple Push Notification service (APNs) VoIP channel for an app	Write	channel*		
UpdateApnsVoipSandboxChannel	Grants permission to update the Apple Push Notification service (APNs) VoIP sandbox channel for an app	Write	channel*		
UpdateApplicationSettings	Grants permission to update the default settings for an app	Write	app*		
UpdateBaiduChannel	Grants permission to update the Baidu channel for an app	Write	channel*		
UpdateCampaign	Grants permission to update a specific campaign	Write	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEmailChannel	Grants permission to update the email channel for an app	Write	channel*		
UpdateEmailTemplate	Grants permission to update a specific email template under the same version or generate a new version	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateEndpoint	Grants permission to create an endpoint or update the information for an endpoint	Write	endpoint*		
UpdateEndpointsBatch	Grants permission to create or update endpoints as a batch operation	Write	app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGcmChannel	Grants permission to update the Firebase Cloud Messaging (FCM) or Google Cloud Messaging (GCM) API key that allows to send push notifications to your Android app	Write	channel*		
UpdateInAppTemplate	Grants permission to update a specific in-app message template under the same version or generate a new version	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourney	Grants permission to update a specific journey	Write	journey*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateJourneyState	Grants permission to update a specific journey state	Write	journey*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePushTemplate	Grants permission to update a specific push notification template under the same version or generate a new version	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateRecommenderConfiguration	Grants permission to update an Amazon Pinpoint configuration for a recommender model	Write	recommender*		
UpdateSegment	Grants permission to update a specific segment	Write	segment*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSmsChannel	Grants permission to update the SMS channel for an app	Write	channel*		
UpdateSmsTemplate	Grants permission to update a specific sms message template under the same version or generate a new version	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTemplateActiveVersion	Grants permission to update the active version parameter of a specific template	Write	template*		
UpdateVoiceChannel	Grants permission to update the Voice channel for an app	Write	channel*		
UpdateVoiceTemplate	Grants permission to update a specific voice message template under the same version or generate a new version	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
VerifyOTPMessage	Grants permission to check the validity of One-Time Passwords (OTPs)	Write	verify-otp*		

Resource types defined by Amazon Pinpoint

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
app	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}`	aws:ResourceTag/${TagKey}
apps	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/*`	
campaign	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}`	aws:ResourceTag/${TagKey}
journey	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}`	aws:ResourceTag/${TagKey}
journeys	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys`	
segment	`arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/segments/${SegmentId}`	aws:ResourceTag/${TagKey}
template	`arn:${Partition}:mobiletargeting:${Region}:${Account}:templates/${TemplateName}/${TemplateType}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
templates	arn:${Partition}:mobiletargeting:${Region}:${Account}:templates	
recommender	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/${RecommenderId}	
recommenders	arn:${Partition}:mobiletargeting:${Region}:${Account}:recommenders/*	
phone-number-validate	arn:${Partition}:mobiletargeting:${Region}:${Account}:phone/number/validate	
channels	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels	
channel	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/channels/${ChannelType}	
event-stream	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/eventstream	
events	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/events	
messages	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/messages	

Resource types	ARN	Condition keys
verify-otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/verify-otp	
otp	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/otp	
attribute	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/attributes/${AttributeType}	
user	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/users/${UserId}	
endpoint	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/endpoints/${EndpointId}	
import-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/import/${JobId}	
export-job	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/jobs/export/${JobId}	
application-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/kpis/daterange/${KpiName}	
campaign-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/campaigns/${CampaignId}/kpis/daterange/${KpiName}	

Resource types	ARN	Condition keys
journey-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/kpis/daterange/${KpiName}	
journey-execution-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/execution-metrics	
journey-execution-activity-metrics	arn:${Partition}:mobiletargeting:${Region}:${Account}:apps/${AppId}/journeys/${JourneyId}/activities/${JourneyActivityId}/execution-metrics	
reports	arn:${Partition}:mobiletargeting:${Region}:${Account}:reports	

Condition keys for Amazon Pinpoint

Amazon Pinpoint defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the pinpoint service	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the list of all the tag key names present in the request the user makes to the pinpoint service	ArrayOfString

Actions, resources, and condition keys for Amazon Pinpoint Email Service

Amazon Pinpoint Email Service (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by Amazon Pinpoint Email Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfigurationSet	Grants permission to create a configuration set	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateDedicatedIpPool	Grants permission to create a new pool of dedicated IP addresses	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Grants permission to create a new predictive inbox placement test	Write	identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Grants permission to start the process of verifying an email identity	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfigurationSetEventDestination	Grants permission to delete an event destination	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Grants permission to delete a dedicated IP pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentity	Grants permission to delete an email identity that you previously verified	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccount	Grants permission to get information about the email-sending status and capabilities	Read		ses:ApiVersion	
GetBlacklistReports	Grants permission to retrieve a list of the deny lists on which your dedicated IP addresses appear	Read		ses:ApiVersion	
GetConfigurationSet	Grants permission to get information about an existing configuration set	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Grants permission to retrieve a list of event destinations that are associated with a configuration set	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDedicatedIp	Grants permission to get information about a dedicated IP address	Read		ses:ApiVersion	
GetDedicatedIps	Grants permission to list the dedicated IP addresses that are associated with your account	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDeliverabilityDashboardOptions	Grants permission to get the status of the Deliverability dashboard	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Grants permission to retrieve the results of a predictive inbox placement test	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDomainDeliverabilityCampaign	Grants permission to retrieve all the deliverability data for a specific campaign	Read		ses:ApiVersion	
GetDomainStatisticsReport	Grants permission to retrieve inbox placement and engagement rates for the domains that you use to send email	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentity	Grants permission to get information about a specific identity associated with your account	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Grants permission to list all of the configuration sets associated with your account	List		ses:ApiVersion	
ListDedicatedIpPools	Grants permission to list all of the dedicated IP pools that exist in your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeliverabilityTestReports	Grants permission to retrieve a list of the predictive inbox placement tests that you've performed, regardless of their statuses	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Grants permission to retrieve deliverability data for all the campaigns that used a specific domain to send email during a specified time range	Read		ses:ApiVersion	
ListEmailIdentities	Grants permission to list all of the email identities that are associated with your account	List		ses:ApiVersion	
ListTagsForResource	Grants permission to retrieve a list of the tags (keys and values) that are associated with a specific resource	Read	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccountDedicatedIpWarmupAttributes	Grants permission to enable or disable the automatic warm-up feature for dedicated IP addresses	Write		ses:ApiVersion	
PutAccountSendingAttributes	Grants permission to enable or disable the ability of your account to send email	Write		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Grants permission to associate a configuration set with a dedicated IP pool	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Grants permission to enable or disable collection of reputation metrics for emails that you send using a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurationSetSendingOptions	Grants permission to enable or disable email sending for messages that use a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Grants permission to specify a custom domain to use for open and click tracking elements in email that you send using a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Grants permission to move a dedicated IP address to an existing dedicated IP pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDedicatedIpWarmupAttributes	Grants permission to enable dedicated IP warm up attributes	Write		ses:ApiVersion	
PutDeliverabilityDashboardOption	Grants permission to enable or disable the Deliverability dashboard	Write		ses:ApiVersion	
PutEmailIdentityDkimAttributes	Grants permission to enable or disable DKIM authentication for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Grants permission to enable or disable feedback forwarding for an identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEmailIdentityMailFromAttributes	Grants permission to enable or disable the custom MAIL FROM domain configuration for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
SendEmail	Grants permission to send an email message	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
TagResource	Grants permission to add one or more tags (keys and values) to a specified resource	Tagging	configuration-set		
			dedicated-ip-pool		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	configuration-set		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
				ses:ApiVersion aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConfigurationSetEventDestination	Grants permission to update the configuration of an event destination for a configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Pinpoint Email 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
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
deliverability-test-report	arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}	aws:ResourceTag/${TagKey}
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Pinpoint Email Service

Amazon Pinpoint Email Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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
ses:ApiVersion	Filters actions based on the SES API version	String
ses:FeedbackAddress	Filters actions based on the "Return-Path" address, which specifies where bounces and complaints are sent by email feedback forwarding	String

Condition keys	Description	Type
ses:FromAddress	Filters actions based on the "From" address of a message	String
ses:FromDisplayName	Filters actions based on the "From" address that is used as the display name of a message	String
ses:Recipients	Filters actions based on the recipient addresses of a message, which include the "To", "CC", and "BCC" addresses	ArrayOfString

Actions, resources, and condition keys for Amazon Pinpoint SMS and Voice Service

Amazon Pinpoint SMS and Voice Service (service prefix: `sms-voice`) 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 Pinpoint SMS and Voice Service
- Resource types defined by Amazon Pinpoint SMS and Voice Service
- Condition keys for Amazon Pinpoint SMS and Voice Service

Actions defined by Amazon Pinpoint SMS and Voice Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfigurationSet	Create a new configuration set. After you create the configuration set, you can add one or more event destinations to it.	Write			
CreateConfigurationSetEventDestination	Create a new event destination in a configuration set.	Write			iam:PassRole
DeleteConfigurationSet	Deletes an existing configuration set.	Write			
DeleteConfigurationSetEventDestination	Deletes an event destination in a configuration set.	Write			
GetConfigurationSetEventDestinations	Obtain information about an event destination, including the types of events it reports, the Amazon Resource Name (ARN) of the destination, and the name of the event destination.	Read			
ListConfigurationSets	Return a list of configuration sets. This operation only returns the configuration sets that are associated with your	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	account in the current AWS Region.				
SendVoiceMessage	Create a new voice message and send it to a recipient's phone number.	Write			
UpdateConfigurationSetEventDestination	Update an event destination in a configuration set. An event destination is a location that you publish information about your voice calls to. For example, you can log an event to an Amazon CloudWatch destination when a call fails.	Write			iam:PassRole

Resource types defined by Amazon Pinpoint SMS and Voice Service

Amazon Pinpoint SMS and Voice Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Pinpoint SMS and Voice Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Pinpoint SMS and Voice Service

Pinpoint SMS Voice has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLexicon	Grants permission to delete the specified pronunciation lexicon stored in an AWS 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	Read	lexicon*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	pronunciation lexicon stored in an AWS Region				
GetSpeechSynthesisTask	Grants permission to get information about specific speech synthesis task	Read			
ListLexicons	Grants permission to list the pronunciation lexicons stored in an AWS Region	List			
ListSpeechSynthesisTasks	Grants permission to list requested speech synthesis tasks	List			
PutLexicon	Grants permission to store a pronunciation lexicon in an AWS Region	Write	lexicon*		
StartSpeechSynthesisStream	Grants permission to perform synthesis with bidirectional streaming	Read	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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Price List

AWS Price List (service prefix: `pricing`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Price List
- Resource types defined by AWS Price List
- Condition keys for AWS Price List

Actions defined by AWS Price List

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServices	Grants permission to retrieve service details for all (paginated) services (if serviceCode is not set) or service detail for a particular service (if given serviceCode)	Read			
GetAttributeValues	Grants permission to retrieve all (paginated) possible values for a given attribute	Read			
GetPriceListFileUrl	Grants permission to retrieve the price list file URL for the given parameters	Read			
GetProducts	Grants permission to retrieve all matching products with given search criteria	Read			
ListPriceLists	Grants permission to list all (paginated) eligible price lists for the given parameters	Read			

Resource types defined by AWS Price List

AWS Price List does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Price List, specify `"Resource": "*"` in your policy.

Condition keys for AWS Price List

Price List has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS PricingPlanManager Service

AWS PricingPlanManager Service (service prefix: `pricingplanmanager`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS PricingPlanManager Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateResourcesToSubscription	Grants permission to associate resources with a subscription	Write			
CancelSubscription	Grants permission to cancel a subscription	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelSubscriptionChange	Grants permission to cancel a pending a change for a subscription	Write			
CreateSubscription	Grants permission to create a subscription	Write			
DisassociateResourcesFromSubscription	Grants permission to disassociate resources from a subscription	Write			
GetSubscription	Grants permission to get the details for a subscription	Read			
ListSubscriptions	Grants permission to list subscriptions in your account	Read			
UpdateSubscription	Grants permission to update a subscription	Write			

Resource types defined by AWS PricingPlanManager 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
subscription	arn:${Partition}:pricingplanmanager::${Account}:subscription/${SubscriptionId}	

Condition keys for AWS PricingPlanManager Service

PricingPlanManager has no service-specific context keys that can be used in the Condition element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Private CA Connector for Active Directory

AWS Private CA Connector for Active Directory (service prefix: pca-connector-ad) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Private CA Connector for Active Directory
- Resource types defined by AWS Private CA Connector for Active Directory
- Condition keys for AWS Private CA Connector for Active Directory

Actions defined by AWS Private CA Connector for Active Directory

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnector	Grants permission to create a Connector in your account	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeVpcEndpoints

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDirectoryRegistration	Grants permission to create a DirectoryRegistration in your account	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	ds:AuthorizeApplication ds:DescribeDirectories
CreateServicePrincipalName	Grants permission to create a ServicePrincipalName for a DirectoryRegistration	Write	Directory Registration*		ds:UpdateAuthorizedApplication
CreateTemplate	Grants permission to create a Template for a Connector	Write	Connector*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTemplateGroupAccessControlEntry	Grants permission to create a TemplateGroupAccessControlEntry for a Template	Write	Template*		
DeleteConnector	Grants permission to delete a Connector in your account	Write	Connector*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DeleteDirectoryRegistration	Grants permission to delete a DirectoryRegistration in your account	Write	DirectoryRegistration*		ds:UnauthorizeApplication ds:UpdateAuthorizedApplication
DeleteServicePrincipalName	Grants permission to delete a ServicePrincipalName for a DirectoryRegistration	Write	DirectoryRegistration*		ds:UpdateAuthorizedApplication
DeleteTemplate	Grants permission to delete a Template for a Connector	Write	Template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTemplateGroupAccessControlEntry	Grants permission to delete a TemplateGroupAccessControlEntry for a Template	Write	Template*		
GetConnector	Grants permission to get a Connector in your account	Read	Connector*		
GetDirectoryRegistration	Grants permission to get a DirectoryRegistration in your account	Read	DirectoryRegistration*		
GetServicePrincipalName	Grants permission to get a ServicePrincipalName for a DirectoryRegistration	Read	DirectoryRegistration*		
GetTemplate	Grants permission to get a Template for a Connector	Read	Template*		
GetTemplateGroupAccessControlEntry	Grants permission to get a TemplateGroupAccessControlEntry for a Template	Read	Template*		
ListConnectors	Grants permission to list the Connectors in your account	List			
ListDirectoryRegistrations	Grants permission to list the DirectoryRegistrations in your account	List			
ListServicePrincipalNames	Grants permission to list the ServicePrincipalNames for a DirectoryRegistration	List	DirectoryRegistration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags for a pca-connector-ad resource in your account	Read			
ListTemplateGroupAccessControlEntries	Grants permission to list the TemplateGroupAccessControlEntries for a Template	List	Template*		
ListTemplates	Grants permission to list the Templates for a Connector	List	Connector*		
TagResource	Grants permission to tag a pca-connector-ad resource in your account	Tagging	Connector		
			Directory Registration		
			Template		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a pca-connector-ad resource in your account	Tagging	Connector		
			Directory Registration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Template		
				aws:TagKeys	
UpdateTemplate	Grants permission to update a Template for a Connector	Write	Template*		
UpdateTemplateGroupAccessControlEntry	Grants permission to update a TemplateGroupAccessControlEntry for a Template	Write	Template*		

Resource types defined by AWS Private CA Connector for Active Directory

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
Connector	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}
Directory Registration	`arn:${Partition}:pca-connector-ad:${Region}:${Account}:directory-registration/${DirectoryId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Template	arn:${Partition}:pca-connector-ad:${Region}:${Account}:connector/${ConnectorId}/template/${TemplateId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Private CA Connector for Active Directory

AWS Private CA Connector for Active Directory defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by on the tags associated with the resource	String
aws:TagKeys	Filters access by on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Private CA Connector for SCEP

AWS Private CA Connector for SCEP (service prefix: pca-connector-scep) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Private CA Connector for SCEP

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateChallenge	Grants permission to create a Challenge for a Connector	Write	Connector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnector	Grants permission to create a SCEP Connector in your account	Write		aws:RequestTag/${TagKey} aws:TagKeys	acm-pca:DescribeCertificateAuthority

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					acm-pca:GetCertificate acm-pca:GetCertificateAuthorityCertificate acm-pca:IssueCertificate
DeleteChallenge	Grants permission to delete a Challenge for a Connector	Write	Challenge*		
DeleteConnector	Grants permission to delete a SCEP Connector in your account	Write	Connector*		
GetChallengeMetadata	Grants permission to get a Challenge for a Connector	Read	Challenge*		
GetChallengePassword	Grants permission to get a Challenge password for a Connector	Read	Challenge*		
GetConnector	Grants permission to get a SCEP Connector in your account	Read	Connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChallengeMetadata	Grants permission to list Challenges for a Connector	List			
ListConnectors	Grants permission to list the SCEP Connectors in your account	List			
ListTagsForResource	Grants permission to list the tags for a pca-connector-scep resource in your account	Read			
TagResource	Grants permission to tag a pca-connector-scep resource in your account	Tagging	Challenge		
			Connector		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a pca-connector-scep resource in your account	Tagging	Challenge		
			Connector		
				aws:TagKeys	

Resource types defined by AWS Private CA Connector for SCEP

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
Challenge	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}/challenge/${ChallengeId}`	aws:ResourceTag/${TagKey}
Connector	`arn:${Partition}:pca-connector-scep:${Region}:${Account}:connector/${ConnectorId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Private CA Connector for SCEP

AWS Private CA Connector for SCEP defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Private Certificate Authority

AWS Private Certificate Authority (service prefix: `acm-pca`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Private Certificate Authority

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCertificateAuthority	Grants permission to create an AWS Private CA and its associated private key and configuration	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	Grants permission to create an audit report for an AWS Private CA	Write	certificate-authority*		
CreatePermission	Grants permission to create a permission for an AWS Private CA	Permissions management	certificate-authority*		
DeleteCertificateAuthority	Grants permission to delete an AWS Private CA and its associated private key and configuration	Write	certificate-authority*		
DeletePermission	Grants permission to delete a permission for an AWS Private CA	Permissions management	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicy	Grants permission to delete the policy for an AWS Private CA	Permissions management	certificate-authority*		
DescribeCertificateAuthority	Grants permission to return a list of the configuration and status fields contained in the specified AWS Private CA	Read	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Grants permission to return the status and information about an AWS Private CA audit report	Read	certificate-authority*		
GetCertificate	Grants permission to retrieve an AWS Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority*		
GetCertificateAuthorityCertificate	Grants permission to retrieve an AWS Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority*		
GetCertificateAuthorityCsr	Grants permission to retrieve an AWS Private CA certificate signing request (CSR) for the certificate-authority specified by an ARN	Read	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPolicy	Grants permission to retrieve the policy on an AWS Private CA	Read	certificate-authority*		
ImportCertificateAuthorityCertificate	Grants permission to import an SSL/TLS certificate into AWS Private CA for use as the CA certificate of an AWS Private CA	Write	certificate-authority*		
IssueCertificate	Grants permission to issue an AWS Private CA certificate	Write	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	Grants permission to retrieve a list of the AWS Private CA certificate authority ARNs, and a summary of the status of each CA in the calling account	List			
ListPermissions	Grants permission to list the permissions that have been applied to the AWS Private CA certificate authority	Read	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTags	Grants permission to list the tags that have been applied to the AWS Private CA certificate authority	Read	certificate-authority*		
PutPolicy	Grants permission to put a policy on an AWS Private CA	Permissions management	certificate-authority*		
RestoreCertificateAuthority	Grants permission to restore an AWS Private CA from the deleted state to the state it was in when deleted	Write	certificate-authority*		
RevokeCertificate	Grants permission to revoke a certificate issued by an AWS Private CA	Write	certificate-authority*		
TagCertificateAuthority	Grants permission to add one or more tags to an AWS Private CA	Tagging	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagCertificateAuthority	Grants permission to remove one or more tags from an AWS Private CA	Tagging	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	Grants permission to update the configuration of an AWS Private CA	Write	certificate-authority*		

Resource types defined by AWS Private Certificate Authority

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Private Certificate Authority

AWS Private Certificate Authority defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
acm-pca:TemplateArn	Filters access by the arn of the certificate template used in Issue Certificate request	ARN
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS PrivateLink

AWS PrivateLink (service prefix: `vpce`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS PrivateLink
- Resource types defined by AWS PrivateLink
- Condition keys for AWS PrivateLink

Actions defined by AWS PrivateLink

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowMultiRegion [permission only]	Grants permission to manage multi-region VPC endpoints and VPC endpoint service configurations	Write	vpc-endpoint		
			vpc-endpoint-service		

Resource types defined by AWS PrivateLink

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
vpc-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint/${VpcEndpointId}`	
vpc-endpoint-service	`arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service/${VpcEndpointServiceId}`	

Condition keys for AWS PrivateLink

VPC Endpoints has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Proton

AWS Proton (service prefix: `proton`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Proton

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptEnvironmentAccountConnection	Grants permission to reject an environment account connection request from another environment account	Write	environment-account-connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelComponentDeployment	Grants permission to cancel component deployment	Write	component*		
CancelEnvironmentDeployment	Grants permission to cancel an environment deployment	Write	environment*		
				proton:EnvironmentTemplate	
CancelServiceInstanceDeployment	Grants permission to cancel a service instance deployment	Write	service-instance*		
				proton:ServiceTemplate	
CancelServicePipelineDeployment	Grants permission to cancel a service pipeline deployment	Write	service*		
				proton:ServiceTemplate	
CreateComponent	Grants permission to create component	Write	component*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironment	Grants permission to create an environment	Write	environment*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} proton:EnvironmentTemplate	
CreateEnvironmentAccountConnection	Grants permission to create an environment account connection	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplate	Grants permission to create an environment template	Write	environment-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMajorVersion	Grants permission to create an environment template major version. DEPRECATED - use CreateEnvironmentTemplateVersion instead	Write	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateEnvironmentTemplateMinorVersion	Grants permission to create an environment template minor version. DEPRECATED - use CreateEnvironmentTemplateVersion instead	Write	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironmentTemplateVersion	Grants permission to create an environment template version	Write	environment-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRepository	Grants permission to create a repository	Write	repository*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateService	Grants permission to create a service	Write	service*		codestar-connections:PassConnection

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceInstance	Grants permission to create a service instance	Write	service-instance*		
				aws:TagKeys aws:RequestTag/${TagKey} proton:ServiceTemplate	
CreateServiceSyncConfig	Grants permission to create a service sync config	Write			
CreateServiceTemplate	Grants permission to create a service template	Write	service-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMajorVersion	Grants permission to create a service template major version. DEPRECATED - use CreateServiceTemplateVersion instead	Write	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateMinorVersion	Grants permission to create a service template minor version. DEPRECATED - use CreateServiceTemplateVersion instead	Write	service-template*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceTemplateVersion	Grants permission to create a service template version	Write	service-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateTemplateSyncConfig	Grants permission to create a template sync config	Write			
DeleteAccountRoles	Grants permission to delete account roles. DEPRECATED - use UpdateAccountSettings instead	Write			
DeleteComponent	Grants permission to delete component	Write	component*		
DeleteDeployment	Grants permission to delete a deployment	Write	deployment*		
DeleteEnvironment	Grants permission to delete an environment	Write	environment*		
				proton:EnvironmentTemplate	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEnvironmentAccountConnection	Grants permission to delete an environment account connection	Write	environment-account-connection*		
DeleteEnvironmentTemplate	Grants permission to delete an environment template	Write	environment-template*		
DeleteEnvironmentTemplateMajorVersion	Grants permission to delete an environment template major version. DEPRECATED - use DeleteEnvironmentTemplateVersion instead	Write	environment-template*		
DeleteEnvironmentTemplateMinorVersion	Grants permission to delete an environment template minor version. DEPRECATED - use DeleteEnvironmentTemplateVersion instead	Write	environment-template*		
DeleteEnvironmentTemplateVersion	Grants permission to delete an environment template version	Write	environment-template*		
DeleteRepository	Grants permission to delete a repository	Write	repository*		
DeleteService	Grants permission to delete a service	Write	service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				proton:ServiceTemplate	
DeleteServiceSyncConfig	Grants permission to delete a service sync config	Write			
DeleteServiceTemplate	Grants permission to delete a service template	Write	service-template*		
DeleteServiceTemplateMajorVersion	Grants permission to delete a service template major version. DEPRECATED - use DeleteServiceTemplateVersion instead	Write	service-template*		
DeleteServiceTemplateMinorVersion	Grants permission to delete a service template minor version. DEPRECATED - use DeleteServiceTemplateVersion instead	Write	service-template*		
DeleteServiceTemplateVersion	Grants permission to delete a service template version	Write	service-template*		
DeleteTemplateSyncConfig	Grants permission to delete a TemplateSyncConfig	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountRoles	Grants permission to get account roles. DEPRECATED - use GetAccountSettings instead	Read			
GetAccountSettings	Grants permission to describe the account settings	Read			
GetComponent	Grants permission to describe a component	Read	component*		
GetDeployment	Grants permission to describe a deployment	Read	deployment*		
GetEnvironment	Grants permission to describe an environment	Read	environment*		
GetEnvironmentAccountConnection	Grants permission to describe an environment account connection	Read	environment-account-connection*		
GetEnvironmentTemplate	Grants permission to describe an environment template	Read	environment-template*		
GetEnvironmentTemplateMajorVersion	Grants permission to get an environment template major version. DEPRECATED - use GetEnvironmentTemplateVersion instead	Read	environment-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEnvironmentTemplateMinorVersion	Grants permission to get an environment template minor version. DEPRECATED - use GetEnvironmentTemplateVersion instead	Read	environment-template*		
GetEnvironmentTemplateVersion	Grants permission to describe an environment template version	Read	environment-template*		
GetRepository	Grants permission to describe a repository	Read	repository*		
GetRepositorySyncStatus	Grants permission to get the latest sync status for a repository	Read			
GetResourceTemplateVersionStatusCounts	Grants permission to list resource template version status counts	Read			
GetResourcesSummary	Grants permission to get resources summary	Read			
GetService	Grants permission to describe a service	Read	service*		
GetServiceInstance	Grants permission to describe a service instance	Read	service-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServiceInstanceSyncStatus	Grants permission to describe the sync status of a service instance	Read			
GetServiceSyncBlockerSummary	Grants permission to describe service sync blockers on a service or service instance	Read			
GetServiceSyncConfig	Grants permission to describe a service sync config	Read			
GetServiceTemplate	Grants permission to describe a service template	Read	service-template*		
GetServiceTemplateMajorVersion	Grants permission to get a service template major version. DEPRECATED - use GetServiceTemplateVersion instead	Read	service-template*		
GetServiceTemplateMinorVersion	Grants permission to get a service template minor version. DEPRECATED - use GetServiceTemplateVersion instead	Read	service-template*		
GetServiceTemplateVersion	Grants permission to describe a service template version	Read	service-template*		
GetTemplateSyncConfig	Grants permission to describe a TemplateSyncConfig	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTemplateSyncStatus	Grants permission to describe the sync status of a template	Read			
ListComponentOutputs	Grants permission to list component outputs	List	component*		
			deployment		
ListComponentProvisionedResources	Grants permission to list component provisioned resources	List	component*		
ListComponents	Grants permission to list components	List	environment		
			service		
			service-instance		
ListDeployments	Grants permission to list deployments	List			
ListEnvironmentAccountConnections	Grants permission to list environment account connections	List			
ListEnvironmentOutputs	Grants permission to list environment outputs	List	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deployment		
ListEnvironmentProvisionedResources	Grants permission to list environment provisioned resources	List	environment*		
ListEnvironmentTemplateMajorVersions	Grants permission to list environment template major versions. DEPRECATED - use ListEnvironmentTemplateVersions instead	List	environment-template*		
ListEnvironmentTemplateMinorVersions	Grants permission to list an environment template minor versions. DEPRECATED - use ListEnvironmentTemplateVersions instead	List	environment-template*		
ListEnvironmentTemplateVersions	Grants permission to list environment template versions	List	environment-template*		
ListEnvironmentTemplates	Grants permission to list environment templates	List			
ListEnvironments	Grants permission to list environments	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRepositories	Grants permission to list repositories	List			
ListRepositorySyncDefinitions	Grants permission to list repository sync definitions	List			
ListServiceInstanceOutputs	Grants permission to list service instance outputs	List	service*		
			service-instance*		
			deployment		
ListServiceInstanceProvisionedResources	Grants permission to list service instance provisioned resources	List	service*		
			service-instance*		
ListServiceInstances	Grants permission to list service instances	List			
ListServicePipelineOutputs	Grants permission to list service pipeline outputs	List	service*		
			deployment		
ListServicePipelineProvisionedResources	Grants permission to list service pipeline provisioned resources	List	service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServiceTemplateMajorVersions	Grants permission to list service template major versions. DEPRECATED - use ListServiceTemplateVersions instead	List	service-template*		
ListServiceTemplateMinorVersions	Grants permission to list service template minor versions. DEPRECATED - use ListServiceTemplateVersions instead	List	service-template*		
ListServiceTemplateVersions	Grants permission to list service template versions	List	service-template*		
ListServiceTemplates	Grants permission to list service templates	List			
ListServices	Grants permission to list services	List			
ListTagsForResource	Grants permission to list tags of a resource	Read	component		
			environment		
			environment-account-connection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		
			service-instance		
			service-template		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
NotifyResourceDeploymentStatusChange	Grants permission to notify Proton of resource deployment status changes	Write	environment		
			service-instance		
RejectEnvironmentAccountConnection	Grants permission to reject an environment account connection request from another environment account	Write	environment-account-connection*		
TagResource	Grants permission to add tags to a resource	Tagging	component		
			environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	component		
			environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment-account-connection		
			environment-template		
			environment-template-major-version		
			environment-template-minor-version		
			environment-template-version		
			repository		
			service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service-instance		
			service-template		
			service-template-major-version		
			service-template-minor-version		
			service-template-version		
				aws:TagKeys	
UpdateAccountRoles	Grants permission to update account roles. DEPRECATED - use UpdateAccountSettings instead	Write			iam:PassRole
UpdateAccountSettings	Grants permission to update the account settings	Write			iam:PassRole
UpdateComponent	Grants permission to update component	Write	component*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update an environment	Write	environment*		iam:PassRole
				proton:EnvironmentTemplate	
UpdateEnvironmentAccountConnection	Grants permission to update an environment account connection	Write	environment-account-connection*		
UpdateEnvironmentTemplate	Grants permission to update an environment template	Write	environment-template*		
UpdateEnvironmentTemplateMajorVersion	Grants permission to update an environment template major version. DEPRECATED - use UpdateEnvironmentTemplateVersion instead	Write	environment-template*		
UpdateEnvironmentTemplateMinorVersion	Grants permission to update an environment template minor version. DEPRECATED - use UpdateEnvironmentTemplateVersion instead	Write	environment-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironmentTemplateVersion	Grants permission to update an environment template version	Write	environment-template*		
UpdateService	Grants permission to update a service	Write	service*		
				proton:ServiceTemplate	
UpdateServiceInstance	Grants permission to update a service instance	Write	service-instance*		
				proton:ServiceTemplate	
UpdateServicePipeline	Grants permission to update a service pipeline	Write	service*		
				proton:ServiceTemplate	
UpdateServiceSyncBlocker	Grants permission to update a service sync blocker	Write			
UpdateServiceSyncConfig	Grants permission to update a service sync config	Write			
UpdateServiceTemplate	Grants permission to update a service template	Write	service-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceTemplateMajorVersion	Grants permission to update a service template major version. DEPRECATED - use UpdateServiceTemplateVersion instead	Write	service-template*		
UpdateServiceTemplateMinorVersion	Grants permission to create a service template minor version. DEPRECATED - use UpdateServiceTemplateVersion instead	Write	service-template*		
UpdateServiceTemplateVersion	Grants permission to update a service template version	Write	service-template*		
UpdateTemplateSyncConfig	Grants permission to update a TemplateSyncConfig	Write			

Resource types defined by AWS Proton

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-template	arn:${Partition}:proton:${Region}:${Account}:environment-template/${Name}	aws:ResourceTag/${TagKey}
environment-template-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
environment-template-major-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
environment-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:environment-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}
service-template	arn:${Partition}:proton:${Region}:${Account}:service-template/${Name}	aws:ResourceTag/${TagKey}
service-template-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersion}.${MinorVersion}	aws:ResourceTag/${TagKey}
service-template-major-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}	aws:ResourceTag/${TagKey}
service-template-minor-version	arn:${Partition}:proton:${Region}:${Account}:service-template/${TemplateName}:${MajorVersionId}.${MinorVersionId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
environment	arn:${Partition}:proton:${Region}:${Account}:environment/${Name}	aws:ResourceTag/${TagKey}
service	arn:${Partition}:proton:${Region}:${Account}:service/${Name}	aws:ResourceTag/${TagKey}
service-instance	arn:${Partition}:proton:${Region}:${Account}:service/${ServiceName}/service-instance/${Name}	aws:ResourceTag/${TagKey}
environment-account-connection	arn:${Partition}:proton:${Region}:${Account}:environment-account-connection/${Id}	aws:ResourceTag/${TagKey}
repository	arn:${Partition}:proton:${Region}:${Account}:repository/${Provider}:${Name}	aws:ResourceTag/${TagKey}
component	arn:${Partition}:proton:${Region}:${Account}:component/${Id}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:proton:${Region}:${Account}:deployment/${Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS Proton

AWS Proton defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys in the request	ArrayOfString
proton:EnvironmentTemplate	Filters access by specified environment template related to resource	String
proton:ServiceTemplate	Filters access by specified service template related to resource	String

Actions, resources, and condition keys for AWS Purchase Orders Console

AWS 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 AWS Purchase Orders Console
- Resource types defined by AWS Purchase Orders Console
- Condition keys for AWS Purchase Orders Console

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPurchaseOrder [permission only]	Grants permission to add a new purchase order	Write	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [permission only]	Grants permission to delete a purchase order	Write	purchase-order*		
				aws:ResourceTag/${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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [permission only]	Grants permission to remove tags from a purchase order	Tagging	purchase-order*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [permission only]	Grants permission to change whether existing or fine-grained IAM actions will be used to control authorization to Billing, Cost Management, and Account consoles	Write			
UpdatePurchaseOrder [permission only]	Grants permission to update an existing purchase order	Write	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus [permission only]	Grants permission to set purchase order status	Write	purchase-order*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ViewPurchaseOrders [permission only]	Grants permission to view purchase orders and details	Read	purchase-order		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS 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 AWS Purchase Orders Console

AWS 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 AWS 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 Q

Amazon Q (service prefix: q) 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 Q
- Resource types defined by Amazon Q
- Condition keys for Amazon Q

Actions defined by Amazon Q

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Connector Resource [permission only]	Grants permission to associate an AWS resource with an Amazon Q connector	Write			
CreateAssignment [permission only]	Grants permission to create a user or group assignment for an Amazon Q Developer Profile	Write	profile*		
				identitystore:UserId identitystore:GroupId	
CreateAuthGrant [permission only]	Grants permission to create OAuth user in Amazon Q	Write			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreateOAuthAppConnection	Grants permission to register an OAuth application in Amazon Q	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
CreatePlugin [permission only]	Grants permission to create and configure a third party plugin in Amazon Q	Write	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAssignment [permission only]	Grants permission to delete a user or group assignment for an Amazon Q Developer Profile	Write	profile*		
				identitystore:UserId identitystore:GroupId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConversation [permission only]	Grants permission to delete a conversation with Amazon Q	Write			
DeleteOAuthAppConnection [permission only]	Grants permission to delete an OAuth application in Amazon Q	Write			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
DeletePlugin [permission only]	Grants permission to delete a configured plugin in Amazon Q	Write	plugin*		
				aws:ResourceTag/${TagKey}	
GenerateCodeFromCommands [permission only]	Grants permission to generate code from CLI commands in Amazon Q	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateCodeRecommendations [permission only]	Grants permission to generate code recommendations in Amazon Q	Read			
GetConnector [permission only]	Grants permission to view information about a specific Amazon Q connector	Read			
GetConversation [permission only]	Grants permission to get individual messages associated with a specific conversation with Amazon Q	Read			
GetIdentityMetadata [permission only]	Grants permission to Amazon Q to get the identity metadata	Read			
GetPlugin [permission only]	Grants permission to view information about a specific configured Amazon Q plugin	Read	plugin*		
				aws:ResourceTag/${TagKey}	
GetTroubleshootingResults [permission only]	Grants permission to get troubleshooting results with Amazon Q	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConversations [permission only]	Grants permission to list individual conversations associated with a specific Amazon Q user	Read			
ListDashboardMetrics [permission only]	Grants permission to read metrics to populate Amazon Q dashboard	List			
ListPluginProviders [permission only]	Grants permission to list available plugins in Amazon Q	List			
ListPlugins [permission only]	Grants permission to list configured plugins in Amazon Q	List	plugin*		
ListTagsForResource [permission only]	Grants permission to list all tags associated with an Amazon Q resource	List	plugin		
				aws:ResourceTag/${TagKey}	
PassRequest [permission only]	Grants permission to allow Amazon Q to perform actions on your behalf	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectConnector [permission only]	Grants permission to reject a connection request for an Amazon Q connector	Write			
SendEvent [permission only]	Grants permission to trigger asynchronous Amazon Q actions	Write			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
SendMessage [permission only]	Grants permission to send a message to Amazon Q	Write			
StartConversation [permission only]	Grants permission to start a conversation with Amazon Q	Write			
StartTroubleshootingAnalysis [permission only]	Grants permission to start a troubleshooting analysis with Amazon Q	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTroubleshootingResolutionExplanation [permission only]	Grants permission to start a troubleshooting resolution explanation with Amazon Q	Write			
TagResource [permission only]	Grants permission to associate tags with an Amazon Q resource	Tagging	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [permission only]	Grants permission to remove tags associated with an Amazon Q resource	Tagging	plugin		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAuthGrant [permission only]	Grants permission to update OAuth user in Amazon Q	Write			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo
UpdateConversation [permission only]	Grants permission to update a conversation with Amazon Q	Write			
UpdateOAuthAppConnection [permission only]	Grants permission to update an OAuth application in Amazon Q	Write			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePlugin [permission only]	Grants permission to update a third party plugin in Amazon Q	Write	plugin*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTroubleshootingCommandResult [permission only]	Grants permission to update a troubleshooting command result with Amazon Q	Write			
UsePlugin [permission only]	Grants permission to use Amazon Q plugins	Write	plugin*		
VerifyOAuthAppConnection [permission only]	Grants permission to verify an OAuth application in Amazon Q	Write			kms:Decrypt kms:GenerateDataKeyWithoutPlaintext kms:ReEncryptFrom kms:ReEncryptTo

Resource types defined by Amazon Q

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:${Partition}:codewhisperer:${Region}:${Account}:profile/${Identifier}`	
plugin	`arn:${Partition}:qdeveloper:${Region}:${Account}:plugin/${Identifier}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Q

Amazon Q defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the Amazon Q resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Condition keys	Description	Type
identitystore:GroupId	Filters access by IAM Identity Center Group ID	ArrayOfString
identitystore:UserId	Filters access by IAM Identity Center User ID	ArrayOfString

Actions, resources, and condition keys for Amazon Q Business

Amazon Q Business (service prefix: `qbusiness`) 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 Q Business
- Resource types defined by Amazon Q Business
- Condition keys for Amazon Q Business

Actions defined by Amazon Q Business

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeli	Grants permission to configure vended log delivery	Permissions	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
veryForResource [permission only]	for Amazon Q Business application resource	management		aws:ResourceTag/${TagKey}	
AssociatePermission	Grants permission to associate resource based policy statement to the application	Write	application*		qbusiness:PutResourcePolicy
BatchDeleteDocument	Grants permission to batch delete document	Write	application*		
			index*		
BatchPutDocument	Grants permission to batch put document	Write	application*		
			index*		
CancelSubscription	Grants permission to cancel a subscription	Write	application*		
			subscription*		
Chat	Grants permission to chat using an application	Read	application*		
ChatSync	Grants permission to chat synchronously using an application	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckDocumentAccess	Grants permission to check if a user has access to a document	Read	application*		
			index*		
CreateAnonymousWebExperienceUrl	Grants permission to create a unique URL for anonymous Amazon Q Business web experience	Write	application*		
			web-experience*		
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateChatResponseConfiguration	Grants permission to create a chat response configuration to the application	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataAccessor	Grants permission to create DataAccessor to the application	Write	application*		qbusiness:CreateDataAccessorWithTti
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAccessorWithTti [permission only]	Grants permission to create AWS IAM Identity center Trusted Token Issuer based DataAccessor to the application	Write	application*		
CreateDataSource	Grants permission to create a data source for a given application and index	Write	application*		
			index*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIndex	Grants permission to create an index for a given application	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegration	Grants permission to create a new integration for a Q Business application	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlugin	Grants permission to create a plugin for a given application	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRetriever	Grants permission to create a retriever for a given application	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Grants permission to create a subscription	Write	application*		
				identitystore:UserId identitystore:GroupId	
CreateUser	Grants permission to create a user	Write	application*		
CreateWebExperience	Grants permission to create a web experience for a given application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Grants permission to delete an application	Write	application*		
DeleteAttachment	Grants permission to delete an attachment in the current chat context	Write	application*		
DeleteChatControlsConfiguration	Grants permission to delete chat controls configuration for an application	Write	application*		
DeleteChatResponseConfiguration	Grants permission to delete a chat response configuration	Write	application*		
			chat-response-configuration*		
DeleteConversation	Grants permission to delete a conversation	Write	application*		
DeleteDataAccessor	Grants permission to delete DataAccessor	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-accessor*		
DeleteDataSource	Grants permission to delete a DataSource	Write	application*		
			data-source*		
			index*		
DeleteGroup	Grants permission to delete a group	Write	application*		
			index*		
DeleteIndex	Grants permission to delete an index	Write	application*		
			index*		
DeleteIntegration	Grants permission to delete an integration for a Q Business application	Write	application*		
			integration*		
DeletePlugin	Grants permission to delete a plugin	Write	application*		
			plugin*		
DeleteRetriever	Grants permission to delete a retriever	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			retriever*		
DeleteUser	Grants permission to delete a user	Write	application*		
DeleteWebExperience	Grants permission to delete a web-experience	Write	application*		
			web-experience*		
DisableAclOnDataSource [permission only]	Grants permission to disable the ACL crawl while creating the Amazon Q Business data source resource	Write	application*		
DisassociatePermission	Grants permission to disassociate resource based policy statement to the application	Write	application*		qbusiness:PutResourcePolicy
GetApplication	Grants permission to get an application	Read	application*		
GetChatControlsConfiguration	Grants permission to get chat controls configuration for an application	List	application*		
GetChatResponseConfiguration	Grants permission to get a chat response configuration	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			chat-response-configuration*		
GetDataAccessor	Grants permission to get DataAccessor	Read	application*		
			data-accessor*		
GetDataSource	Grants permission to get a data source	Read	application*		
			data-source*		
			index*		
GetDocumentContent	Grants permission to get a document content	Read	application*		
			index*		
GetGroup	Grants permission to get a group	Read	application*		
			index*		
GetIndex	Grants permission to get an index	Read	application*		
			index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIntegration	Grants permission to get an integration for a Q Business application	Read	application*		
			integration*		
GetMedia	Grants permission to get the media associated to a system message	Read	application*		
GetPlugin	Grants permission to get a plugin	Read	application*		
			plugin*		
GetPolicy	Grants permission to get resource based policy of the application	Read	application*		
GetRetriever	Grants permission to get a retriever	Read	application*		
			retriever*		
GetUser	Grants permission to get a user	Read	application*		
GetWebExperience	Grants permission to get a web-experience	Read	application*		
			web-experience*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Grants permission to list the applications	List			
ListAttachments	Grants permission to list attachments in the current chat context	List	application*		
ListChatResponseConfigurations	Grants permission to list chat response configurations for an application	List	application*		
ListConversations	Grants permission to list all conversations for an application	List	application*		
ListDataAccessors	Grants permission to list DataAccessors for the application	List	application*		
ListDataSourceSyncJobs	Grants permission to get Data Source sync job history	List	application*		
			data-source*		
			index*		
ListDataSources	Grants permission to list the data sources of an application and an index	List	application*		
			index*		
ListDocuments	Grants permission to list all documents	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			index*		
ListGroups	Grants permission to list groups	List	application*		
			index*		
ListIndices	Grants permission to list the indices of an application	List	application*		
ListIntegrations	Grants permission to list all integrations for a Q Business application	List	application*		
ListMessages	Grants permission to list all messages	List	application*		
ListPluginActions	Grants permission to list the plugins actions of a plugin within application	Read	application*		
			plugin*		
ListPluginTypeActions	Grants permission to list all the actions for a plugin type	Read			
ListPluginTypeMetadata	Grants permission to list all the plugin type metadata	Read			
ListPlugins	Grants permission to list the plugins of an application	List	application*		
ListRetrievers	Grants permission to list the retrievers of an application	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSubscriptions	Grants permission to list subscriptions	List	application*		
ListTagsForResource	Grants permission to list tags for a resource	Read	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		
ListWebExperiences	Grants permission to list the web experiences of an application	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFeedback	Grants permission to put feedback about a conversation message	Write	application*		
PutGroup	Grants permission to put a group of users	Write	application*		
			index*		
PutResourcePolicy [permission only]	Grants permission to put resource based policy statement to the application	Write	application*		
SearchRelevantContent	Grants permission to search relevant content from the Amazon Q Business Application	Read	application*		
StartDataSourceSyncJob	Grants permission to start Data Source sync job	Write	application*		
			data-source*		
			index*		
StartDeployment	Grants permission to start deployment for an integration	Write	application*		
			integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopDataSourceSyncJob	Grants permission to stop Data Source sync job	Write	application*		
			data-source*		
			index*		
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	application		
			chat-response-configuration		
			data-accessor		
			data-source		
			index		
			integration		
			plugin		
			retriever		
			web-experience		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateApplication	Grants permission to update an Application	Write	application*		
UpdateChatControlsConfiguration	Grants permission to update chat controls configuration for an application	Write	application*		
UpdateChatResponseConfiguration	Grants permission to update a chat response configuration	Write	application*		
			chat-response-configuration*		
UpdateDataAccessor	Grants permission to update DataAccessor	Write	application*		
			data-accessor*		
UpdateDataSource	Grants permission to update a DataSource	Write	application*		
			data-source*		
			index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIndex	Grants permission to update an index	Write	application*		
			index*		
UpdateIntegration	Grants permission to update an integration for a Q Business application	Write	application*		
			integration*		
UpdatePlugin	Grants permission to update a plugin	Write	application*		
			plugin*		
UpdateRetriever	Grants permission to update a Retriever	Write	application*		
			retriever*		
UpdateSubscription	Grants permission to update a subscription	Write	application*		
			subscription*		
UpdateUser	Grants permission to update a user	Write	application*		
UpdateWebExperience	Grants permission to update a WebExperience	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			web-experience*		

Resource types defined by Amazon Q Business

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:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	aws:ResourceTag/${TagKey}
integration	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/integration/${IntegrationId}`	aws:ResourceTag/${TagKey}
retriever	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/retriever/${RetrieverId}`	aws:ResourceTag/${TagKey}
index	`arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
data-source	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/index/${IndexId}/data-source/${DataSourceId}	aws:ResourceTag/${TagKey}
plugin	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/plugin/${PluginId}	aws:ResourceTag/${TagKey}
web-experience	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/web-experience/${WebExperienceId}	aws:ResourceTag/${TagKey}
subscription	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/subscription/${SubscriptionId}	
data-accessor	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/data-accessor/${DataAccessorId}	aws:ResourceTag/${TagKey}
chat-response-configuration	arn:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}/chat-response-configuration/${ChatResponseConfigurationId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Q Business

Amazon Q Business defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
identitystore:GroupId	Filters access by IAM Identity Center Group ID	ArrayOfString
identitystore:UserId	Filters access by IAM Identity Center User ID	ArrayOfString

Actions, resources, and condition keys for Amazon Q Business Q Apps

Amazon Q Business Q Apps (service prefix: qapps) 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 Q Business Q Apps
- Resource types defined by Amazon Q Business Q Apps
- Condition keys for Amazon Q Business Q Apps

Actions defined by Amazon Q Business Q Apps

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateLibraryItemReview	Grants permission to associate a library item review in the Q Business application environment	Write	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
AssociateQAppWithUser	Grants permission to associate Q App with a user in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
BatchCreateCategory	Grants permission to create the categories of a library in the Q Business application environment	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteCategory	Grants permission to delete the categories of a library in the Q Business application environment	Write	application*		
BatchUpdateCategory	Grants permission to update the categories of a library in the Q Business application environment	Write	application*		
CopyQApp [permission only]	Grants permission to copy Q App in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItem	Grants permission to create a library item in the Q Business application environment	Write	application		
			qapp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateLibraryItemReview [permission only]	Grants permission to create a library item review in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
CreateQApp	Grants permission to create Q App in the Q Business application environment	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubscriptionToken [permission only]	Grants permission to subscribe to a Q App event bus topic in the Q Business application environment	Write	application*		
DeleteLibraryItem	Grants permission to delete a library item in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DeleteQApp	Grants permission to delete Q App in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeQAppPermissions	Grants permission to get Q App sharing permissions in the Q Business application environment	Read	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateLibraryItemReview	Grants permission to disassociate a library item review in the Q Business application environment	Write	qapp*		
				qapps:UserIsAppOwner qapps:AppIsPublished	
DisassociateQAppFromUser	Grants permission to disassociate Q App with a user in the Q Business application environment	Write	application		
			qapp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				qapps:UserIsAppOwner qapps:AppIsPublished	
ExportQAppSessionData	Grants permission to export Q App session data in the Q Business application environment	Write	qapp-session*		
GetLibraryItem	Grants permission to get a library item in the Q Business application environment	Read	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQApp	Grants permission to get Q App in the Q Business application environment	Read	application		
			qapp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				qapps:UserIsAppOwner qapps:AppIsPublished	
GetQAppSession	Grants permission to get Q App session in the Q Business application environment	Read	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
GetQAppSessionMetadata	Grants permission to get Q App session metadata in the Q Business application environment	Read	qapp-session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportDocument	Grants permission to import a document to Q App or Q App Session in the Q Business application environment	Write	qapp		
			qapp-session		
				qapps:UserIsAppOwner	
				qapps:AppIsPublished	
				qapps:UserIsSessionModerator	
				qapps:SessionIsShared	
ListCategories	Grants permission to list categories in the Q Business application environment	List	application*		
ListLibraryItems	Grants permission to list library items in the Q Business application environment	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListQAppSessionData	Grants permission to get Q App session data in the Q Business application environment	Read	qapp-session*		
ListQApps	Grants permission to list Q Apps in the Q Business application environment	List	application*		
ListTagsForResource	Grants permission to list tags for a resource	Read	qapp		
			qapp-session		
PredictProblemStatementFromConversation [permission only]	Grants permission to predict problem statement from conversation log in the Q Business application environment	Write	application*		
PredictQApp	Grants permission to predict Q App from conversation log or problem statement in the Q Business application environment	Write	application*		
PredictQAppFromProblemStatement [permission only]	Grants permission to predict Q App metadata from problem statement in the Q Business application environment	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartQAppSession	Grants permission to start Q App session in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished aws:RequestTag/${TagKey} aws:TagKeys	
StopQAppSession	Grants permission to stop Q App session in the Q Business application environment	Write	application		
			qapp-session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	qapp		
			qapp-session		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the tag with the given key from a resource	Tagging	qapp		
			qapp-session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateLibraryItem	Grants permission to update a library item in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateLibraryItemMetadata	Grants permission to update the metadata of a library item in the Q Business application environment	Write	qapp*		
				qapps:AppIsPublished	
UpdateQApp	Grants permission to update Q App in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateQAppPermissions	Grants permission to update Q App sharing permissions in the Q Business application environment	Write	application		
			qapp		
				qapps:UserIsAppOwner qapps:AppIsPublished	
UpdateQAppSession	Grants permission to update Q App session in the Q Business application environment	Write	qapp-session*		
				qapps:UserIsAppOwner qapps:AppIsPublished qapps:UserIsSessionModerator qapps:SessionIsShared	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateQAppSessionMetadata	Grants permission to update Q App session metadata in the Q Business application environment	Write	qapp-session*		

Resource types defined by Amazon Q Business Q Apps

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:${Partition}:qbusiness:${Region}:${Account}:application/${ApplicationId}`	
qapp	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}`	aws:ResourceTag/${TagKey}
qapp-session	`arn:${Partition}:qapps:${Region}:${Account}:application/${ApplicationId}/qapp/${AppId}/session/${SessionId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Q Business Q Apps

Amazon Q Business Q Apps defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
qapps:AppIsPublished	Filters access by whether Q App is published	String
qapps:SessionIsShared	Filters access by whether Q App Session is shared	String
qapps:UserIsAppOwner	Filters access by whether requester is Q App owner	String
qapps:UserIsSessionModerator	Filters access by whether requester is Q App Session moderator	String

Actions, resources, and condition keys for Amazon Q Developer

Amazon Q Developer (service prefix: `qdeveloper`) 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 Q Developer

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportArtifact	Grants permission to export artifacts from Amazon Q Developer	Write	codeTransformation		
ImportArtifact	Grants permission to import artifacts to Amazon Q Developer	Write	codeTransformation		
ListTagsForResource [permission only]	Grants permission to list all tags associated with an Amazon Q Developer resource	List	codeTransformation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartAgentSession	Grants permission to start an agent session with Amazon Q Developer	Write		aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [permission only]	Grants permission to associate tags with an Amazon Q Developer resource	Tagging	codeTransformation		
				aws:TagKeys aws:RequestTag/${TagKey}	
TransformCode	Grants permission to transform code with Amazon Q Developer Transform Agent	Write	codeTransformation		
UntagResource [permission only]	Grants permission to remove tags associated with an Amazon Q Developer resource	Tagging	codeTransformation		
				aws:TagKeys	

Resource types defined by Amazon Q Developer

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
codeTransformation	`arn:${Partition}:qdeveloper:${Region}:${Account}:codeTransformation/${Identifier}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Q Developer

Amazon Q Developer defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the Amazon Q Developer resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Q in Connect

Amazon Q in Connect (service prefix: `wisdom`) 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 Q in 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateMessageTemplate	Grants permission to activate a message template	Write	KnowledgeBase*		
			MessageTemplate*		
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for an assistant	Permissions management	Assistant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAIAgent	Grants permission to create an ai agent	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIAgentVersion	Grants permission to create an ai agent version	Write	AIAgent*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrail	Grants permission to create an ai guardrail	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIGuardrailVersion	Grants permission to create an ai guardrail version	Write	AIGuardrail*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPrompt	Grants permission to create an ai prompt	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateAIPromptVersion	Grants permission to create an ai prompt version	Write	AIPrompt*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateAssistant	Grants permission to create an assistant	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAssistantAssociation	Grants permission to create an association between an assistant and another resource	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateContent	Grants permission to create content	Write	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContentAssociation	Grants permission to create a content association	Write	Content*		
			KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKnowledgeBase	Grants permission to create a knowledge base	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplate	Grants permission to create a message template	Write	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateMessageTemplateAttachment	Grants permission to create an attachment to a message template	Write	KnowledgeBase*		
			MessageTemplate*		
CreateMessageTemplateVersion	Grants permission to create a version of a message template	Write	KnowledgeBase*		
			MessageTemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQuickResponse	Grants permission to create quick response	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSession	Grants permission to create a session	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMessageTemplate	Grants permission to deactivate a message template	Write	KnowledgeBase*		
			MessageTemplate*		
DeleteAIAgent	Grants permission to delete an ai agent	Write	AIAgent*		
DeleteAIAgentVersion	Grants permission to delete an ai agent version	Write	AIAgent*		
DeleteAIGuardrail	Grants permission to delete an ai guardrail	Write	AIGuardrail*		
DeleteAIGuardrailVersion	Grants permission to delete an ai guardrail version	Write	AIGuardrail*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAIPrompt	Grants permission to delete an ai prompt	Write	AIPrompt*		
DeleteAIPromptVersion	Grants permission to delete an ai prompt version	Write	AIPrompt*		
DeleteAssistant	Grants permission to delete an assistant	Write	Assistant*		
DeleteAssistantAssociation	Grants permission to delete an assistant association	Write	AssistantAssociation*		
DeleteContent	Grants permission to delete content	Write	Content*		
			KnowledgeBase*		
DeleteContentAssociation	Grants permission to delete a content association	Write	Content*		
			ContentAssociation*		
			KnowledgeBase*		
DeleteImportJob	Grants permission to delete a import job of a knowledge base	Write	KnowledgeBase*		
DeleteKnowledgeBase	Grants permission to delete a knowledge base	Write	KnowledgeBase*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMessageTemplate	Grants permission to delete a message template	Write	KnowledgeBase*		
			MessageTemplate*		
DeleteMessageTemplateAttachment	Grants permission to delete an attachment from a message template	Write	KnowledgeBase*		
			MessageTemplate*		
DeleteQuickResponse	Grants permission to delete quick response	Write	KnowledgeBase*		
			QuickResponse*		
GetAIAgent	Grants permission to retrieve information about an ai agent	Read	AIAgent*		
GetAIGuardrail	Grants permission to retrieve information about an ai guardrail	Read	AIGuardrail*		
GetAIPrompt	Grants permission to retrieve information about an ai prompt	Read	AIPrompt*		
GetAssistant	Grants permission to retrieve information about an assistant	Read	Assistant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssistantAssociation	Grants permission to retrieve information about an assistant association	Read	AssistantAssociation*		
GetContent	Grants permission to retrieve content, including a pre-signed URL to download the content	Read	Content*		
			KnowledgeBase*		
GetContentAssociation	Grants permission to retrieve information about a content association	Read	Content*		
			ContentAssociation*		
			KnowledgeBase*		
GetContentSummary	Grants permission to retrieve summary information about the content	Read	Content*		
			KnowledgeBase*		
GetImportJob	Grants permission to retrieve information about the import job	Read	KnowledgeBase*		
GetKnowledgeBase	Grants permission to retrieve information about the knowledge base	Read	KnowledgeBase*		
GetMessageTemplate	Grants permission to retrieve a message template	Read	KnowledgeBase*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
GetNextMessage	Grants permission to retrieve for next message in a session	Read	Session*		
GetQuickResponse	Grants permission to retrieve content	Read	KnowledgeBase*		
			QuickResponse*		
GetRecommendations	Grants permission to retrieve recommendations for the specified session	Read	Session*		
GetSession	Grants permission to retrieve information for a specified session	Read	Session*		
ListAIAgentVersions	Grants permission to list information about ai agent versions	List	AIAgent*		
ListAIAgents	Grants permission to list information about ai agents	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAIGuardrailVersions	Grants permission to list information about ai guardrail versions	List	AIGuardrail*		
ListAIGuardrails	Grants permission to list information about ai guardrails	List			
ListAIPromptVersions	Grants permission to list information about ai prompt versions	List	AIPrompt*		
ListAIPrompts	Grants permission to list information about ai prompts	List			
ListAssistantAssociations	Grants permission to list information about assistant associations	List			
ListAssistants	Grants permission to list information about assistants	List			
ListContentAssociations	Grants permission to list information about content associations	List	Content* KnowledgeBase*		
ListContents	Grants permission to list the content with a knowledge base	List	KnowledgeBase*		
ListImportJobs	Grants permission to list information about knowledge bases	List	KnowledgeBase*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListKnowledgeBases	Grants permission to list information about knowledge bases	List			
ListMessageTemplateVersions	Grants permission to list message template versions for the specified message template	List	KnowledgeBase*		
			MessageTemplate*		
ListMessageTemplates	Grants permission to list the message templates for a knowledge base	List	KnowledgeBase*		
ListMessages	Grants permission to list messages in a session	List	Session*		
ListQuickResponses	Grants permission to list the quick response with a knowledge base	List	KnowledgeBase*		
ListTagsForResource	Grants permission to list the tags for the specified resource	Read			
NotifyRecommendationsReceived	Grants permission to remove the specified recommendations from the specified assistant's queue of newly available recommendations	Write	Session*		
PutFeedback	Grants permission to submit feedback	Write	Assistant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
QueryAssistant	Grants permission to perform a manual search against the specified assistant	Read	Assistant*		
RemoveAssistantAIAgent	Grants permission to remove an ai agent from an assistant	Write	Assistant*		
RemoveKnowledgeBaseTemplateUri	Grants permission to remove a URI template from a knowledge base	Write	KnowledgeBase*		
RenderMessageTemplate	Grants permission to render a message template	Read	KnowledgeBase*		wisdom:GetMessageTemplate
			MessageTemplate*		
				wisdom:MessageTemplate/RoutingProfileArn	
Retrieve	Grants permission to retrieve knowledge content from specified assistant associations	Read	Assistant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchContent	Grants permission to search for content referencing a specified knowledge base. Can be used to get a specific content resource by its name	Read	KnowledgeBase*		
SearchMessageTemplates	Grants permission to search for message templates referencing a specified knowledge base	Read	KnowledgeBase*		
				wisdom:SearchFilter/RoutingProfileArn wisdom:SearchFilter/Qualifier	
SearchQuickResponses	Grants permission to search for quick response referencing a specified knowledge base	Read	KnowledgeBase*		wisdom:GetQuickResponse
				wisdom:SearchFilter/RoutingProfileArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchSessions	Grants permission to search for sessions referencing a specified assistant. Can be used to et a specific session resource by its name	Read			
SendMessage	Grants permission to send a message	Write	Session*		
StartContentUpload	Grants permission to get a URL to upload content to a knowledge base	Write	KnowledgeBase*		
StartImportJob	Grants permission to create multiple quick responses	Write	KnowledgeBase*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Grants permission to add the specified tags to the specified resource	Tagging	Assistant		
			AssistantAssociation		
			Content		
			ContentAssociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	Assistant		
			AssistantAssociation		
			Content		
			ContentAssociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			KnowledgeBase		
			MessageTemplate		
			QuickResponse		
			Session		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAIAgent	Grants permission to update information about an ai agent	Write	AIAgent*		
UpdateAIGuardrail	Grants permission to update information about an ai guardrail	Write	AIGuardrail*		
UpdateAIPrompt	Grants permission to update information about an ai prompt	Write	AIPrompt*		
UpdateAssistantAIAgent	Grants permission to update assistant information about an ai agent	Write	Assistant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContent	Grants permission to update information about the content	Write	Content*		
			KnowledgeBase*		
UpdateKnowledgeBaseTemplateUri	Grants permission to update the template URI of a knowledge base	Write	KnowledgeBase*		
UpdateMessageTemplate	Grants permission to update content of the message template	Write	KnowledgeBase*		
			MessageTemplate*		
UpdateMessageTemplateMetadata	Grants permission to update metadata of the message template	Write	KnowledgeBase*		
			MessageTemplate*		
UpdateQuickResponse	Grants permission to update information or content of the quick response	Write	KnowledgeBase*		
			QuickResponse*		
UpdateSession	Grants permission to update a session	Write	Session*		
UpdateSessionData	Grants permission to update data stored in a session	Write	Session*		

Resource types defined by Amazon Q in 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
AIAgent	`arn:${Partition}:wisdom:${Region}:${Account}:ai-agent/${AssistantId}/${AIAgentId}`	aws:ResourceTag/${TagKey}
AIPrompt	`arn:${Partition}:wisdom:${Region}:${Account}:ai-prompt/${AssistantId}/${AIPromptId}`	aws:ResourceTag/${TagKey}
AIGuardrail	`arn:${Partition}:wisdom:${Region}:${Account}:ai-guardrail/${AssistantId}/${AIGuardrailId}`	aws:ResourceTag/${TagKey}
Assistant	`arn:${Partition}:wisdom:${Region}:${Account}:assistant/${AssistantId}`	aws:ResourceTag/${TagKey}
Assistant Association	`arn:${Partition}:wisdom:${Region}:${Account}:association/${AssistantId}/${AssistantAssociationId}`	aws:ResourceTag/${TagKey}
Content	`arn:${Partition}:wisdom:${Region}:${Account}:content/${KnowledgeBaseId}/${ContentId}`	aws:ResourceTag/${TagKey}
ContentAssociation	`arn:${Partition}:wisdom:${Region}:${Account}:content-association/${KnowledgeBaseId}/${ContentId}/${ContentAssociationId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Knowledge Base	arn:${Partition}:wisdom:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
MessageTemplate	arn:${Partition}:wisdom:${Region}:${Account}:message-template/${KnowledgeBaseId}/${MessageTemplateId}	aws:ResourceTag/${TagKey} wisdom:MessageTemplate/RoutingProfileArn
Session	arn:${Partition}:wisdom:${Region}:${Account}:session/${AssistantId}/${SessionId}	aws:ResourceTag/${TagKey}
QuickResponse	arn:${Partition}:wisdom:${Region}:${Account}:quick-response/${KnowledgeBaseId}/${QuickResponseId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Q in Connect

Amazon Q in 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
wisdom:MessageTemplate/RoutingProfileArn	Filters access by the connect routing profile arns associated with the resource	ArrayOfARN
wisdom:SearchFilter/Qualifier	Filters access by the qualifiers that are passed in the request	ArrayOfString
wisdom:SearchFilter/RoutingProfileArn	Filters access by the connect routing profile arn that is passed in the request	ARN

Actions, resources, and condition keys for Amazon QLDB

Amazon QLDB (service prefix: `qldb`) 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 QLDB
- Resource types defined by Amazon QLDB

- Condition keys for Amazon QLDB

Actions defined by Amazon QLDB

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelJournalKinesisStream	Grants permission to cancel a journal kinesis stream	Write	stream*		
CreateLedger	Grants permission to create a ledger	Write	ledger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLedger	Grants permission to delete a ledger	Write	ledger*		
DescribeJournalKinesisStream	Grants permission to describe information about a journal kinesis stream	Read	stream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJournalS3Export	Grants permission to describe information about a journal export job	Read	ledger*		
DescribeLedger	Grants permission to describe a ledger	Read	ledger*		
ExecuteStatement [permission only]	Grants permission to send commands to a ledger via the console	Write	ledger*		
ExportJournalToS3	Grants permission to export journal contents to an Amazon S3 bucket	Write	ledger*		
GetBlock	Grants permission to retrieve a block from a ledger for a given BlockAddress	Read	ledger*		
GetDigest	Grants permission to retrieve a digest from a ledger for a given BlockAddress	Read	ledger*		
GetRevision	Grants permission to retrieve a revision for a given document ID and a given BlockAddress	Read	ledger*		
InsertSampleData [permission only]	Grants permission to insert sample application data via the console	Write	ledger*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListJournalKinesisStreamsForLedger	Grants permission to list journal kinesis streams for a specified ledger	List	stream*		
ListJournalS3Exports	Grants permission to list journal export jobs for all ledgers	List			
ListJournalS3ExportsForLedger	Grants permission to list journal export jobs for a specified ledger	List	ledger*		
ListLedgers	Grants permission to list existing ledgers	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	catalog		
			ledger		
			stream		
			table		
PartiQLCreateIndex	Grants permission to create an index on a table	Write	table*		
PartiQLCreateTable	Grants permission to create a table	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
PartiQLDelete	Grants permission to delete documents from a table	Write	table*		
PartiQLDropIndex	Grants permission to drop an index from a table	Write	table*		
				qldb:Purge	
PartiQLDropTable	Grants permission to drop a table	Write	table*		
				qldb:Purge	
PartiQLHistoryFunction	Grants permission to use the history function on a table	Read	table*		
PartiQLInsert	Grants permission to insert documents into a table	Write	table*		
PartiQLRedact	Grants permission to redact historic revisions	Write	table*		
PartiQLSelect	Grants permission to select documents from a table	Read	catalog		
			table		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PartiQLUndropTable	Grants permission to undrop a table	Write	table*		
PartiQLUpdate	Grants permission to update existing documents in a table	Write	table*		
SendCommand	Grants permission to send commands to a ledger	Write	ledger*		
ShowCatalog [permission only]	Grants permission to view a ledger's catalog via the console	Write	ledger*		
StreamJournalToKinesis	Grants permission to stream journal contents to a Kinesis Data Stream	Write	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to add one or more tags to a resource	Tagging	catalog		
			ledger		
			stream		
			table		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	catalog		
			ledger		
			stream		
			table		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateLedger	Grants permission to update properties on a ledger	Write	ledger*		
UpdateLedgerPermissionsMode	Grants permission to update the permissions mode on a ledger	Write	ledger*		

Resource types defined by Amazon QLDB

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
ledger	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}`	aws:ResourceTag/${TagKey}
stream	`arn:${Partition}:qldb:${Region}:${Account}:stream/${LedgerName}/${StreamId}`	aws:ResourceTag/${TagKey}
table	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/table/${TableId}`	aws:ResourceTag/${TagKey}
catalog	`arn:${Partition}:qldb:${Region}:${Account}:ledger/${LedgerName}/information_schema/user_tables`	aws:ResourceTag/${TagKey}

Condition keys for Amazon QLDB

Amazon QLDB defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
qldb:Purge	Filters access by the value of purge that is specified in a PartiQL DROP statement	String

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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccountConfigurations [permission only]	Grants permission to enable setting default access to AWS resources	Write			
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure log delivery for QuickSuite instance	Permissions management			
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} aws:TagKeys	
BatchGetPreferences	Grants permission to get user preferences	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
BatchUpdatePreferences [permission only]	Grants permission to update user preferences	Write			
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateActionConnector	Grants permission to create an action connector	Write	actionconnector*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdmin [permission only]	Grants permission to provision Amazon QuickSight administrators, authors, and readers	Write	user*		
CreateAnalysis	Grants permission to create an analysis from a template	Write	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrand	Grants permission to create an Amazon QuickSight brand	Write	brand*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Grants permission to create a dataset	Write	datasource*		quicksight:PassDataSource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Grants permission to create a data source	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateEmailCustomizationTemplate [permission only]	Grants permission to create a QuickSight email customization template	Write	emailCustomizationTemplate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtensionAccess [permission only]	Grants permission to create an extension access	Write	extensionaccess*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFolder	Grants permission to create a QuickSight folder	Write	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	Grants permission to add a QuickSight Dashboard, Analysis or Dataset to a QuickSight Folder	Write	folder*		
			analysis		
			dashboard		
			dataset		
CreateGroup	Grants permission to create a QuickSight group	Write	group*		
CreateGroupMembership	Grants permission to add a QuickSight user to a QuickSight group	Write	group*	quicksight:UserName	
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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	
CreateTemplate	Grants permission to create a template	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	Grants permission to create an alias for a theme version	Write	theme*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
CreateUser [permission only]	Grants permission to provision Amazon QuickSight authors and readers	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVPCConnection	Grants permission to create a vpc connection	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomPermission	Grants permission to remove the custom permission associated with an account	Write			
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*		
DeleteActionConnector	Grants permission to delete an action connector	Write	actionconnector*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomPermissions	Grants permission to delete a QuickSight custom permissions resource	Write			
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDefaultQBusinessApplication	Grants permission to delete linked QBusiness application for QuickSight account	Write			
DeleteEmailCustomizationTemplate [permission only]	Grants permission to delete a QuickSight email customization template	Write	emailCustomizationTemplate*		
DeleteExtensionAccess [permission only]	Grants permission to delete an extension access	Write	extensionaccess*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS services for trusted identity propagation in QuickSight	Write			
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	
DeleteTemplate	Grants permission to delete a template	Write	template*		
DeleteTemplateAlias	Grants permission to delete a template alias	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				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 delete 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAccountCustomPermission	Grants permission to describe the custom permission associated with an account	Read			
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*		
DescribeActionConnector	Grants permission to describe an action connector	Read	actionconnector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeActionConnectorPermissions	Grants permission to describe permissions for an action connector	Read	actionconnector*		
DescribeAgent [permission only]	Grants permission to describe an agent	Read	agent*		
DescribeAgentPermissions [permission only]	Grants permission to describe agent's permissions	Read	agent*		
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*		
DescribeChatConfiguration [permission only]	Grants permission to describe chat configuration	Read			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDashboardSnapshotJobResult	Grants permission to describe result of a dashboard snapshot job	Read	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	Grants permission to describe dashboards qa configuration	Read			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDataSource	Grants permission to describe a data source	Read	datasource*		
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeExtensionAccess [permission only]	Grants permission to describe an extension access	Read	extensionaccess*		
DescribeFolder	Grants permission to describe a QuickSight Folder	Read	folder*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	Grants permission to describe the IP restrictions for QuickSight account	Read			
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			
DescribeQuickIndexCapacity [permission only]	Grants permission to describe index capacity	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeSelfUpgradeConfiguration	Grants permission to describe the administrative self upgrade configuration associated with an account	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*		
DescribeTheme	Grants permission to describe a theme	Read	theme*		
DescribeThemeAlias	Grants permission to describe a theme alias	Read	theme*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			topic		
				quicksight:AllowedEmbeddingDomains	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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*		
GetCustomPermissionsSummary [permission only]	Grants permission to get information about the custom permissions in an account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDashboardEmbedUrl	Grants permission to get a URL used to embed a QuickSight Dashboard	Read	dashboard*		
GetFlowMetadata	Grants permission to get metadata for a flow	Read	flow*		
GetFlowPermissions	Grants permission to get permissions for a flow	Read	flow*		
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			
GetIdentityContext	Grants permission to get identity context for a user	Read	user*		
GetSessionEmbedUrl	Grants permission to get a URL to embed QuickSight console experience	Read			
ListActionConnectors	Grants permission to list action connectors	List			
ListAgents [permission only]	Grants permission to list agents	List	agent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAnalyses	Grants permission to list all analyses in an account	List	analysis*		
ListAssetBundleExportJobs	Grants permission to list all asset bundle export jobs	List	assetBundleExportJob*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataSets	Grants permission to list all datasets	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListDataSources	Grants permission to list all data sources	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListExtensionAccesses [permission only]	Grants permission to list extension accesses	List			
ListFlows	Grants permission to list all flows in an Amazon QuickSight account	List			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 AWS services enabled for trusted identity propagation in QuickSight	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListRefreshSchedules	Grants permission to list all refresh schedules on a dataset	List			
ListRoleMemberships	Grants permission to list the members of a role	List			
ListSelfUpgrades	Grants permission to list all of the pending self upgrade requests associated with an account	List	user*		
ListTagsForResource	Grants permission to list tags of a QuickSight resource	Read	actionconnector analysis		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			emailCustomizationTemplate		
			flow		
			folder		
			template		
			theme		
			topic		
			vpcconnection		
ListTemplateAliases	Grants permission to list all aliases for a template	List	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
QuickSuiteUsageMetrics [permission only]	Grants permission to get QuickSuite usage metrics	Read			
RegisterCustomerManagedKey [permission only]	Grants permission to register a customer managed key	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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 AWS resources	Write			
SearchActionConnectors	Grants permission to search action connectors	List	actionconnector*		
SearchAgents [permission only]	Grants permission to search agents	List	agent*		
SearchAnalyses	Grants permission to search for a sub-set of analyses	List	analysis*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			
SearchFlows	Grants permission to search flows in an Amazon QuickSight account	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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	actionconnector		
			analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			emailCustomizationTemplate		
			flow		
			folder		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
Unpublish Flow [permission only]	Grants permission to unpublish a flow	Write	flow*		
Unsubscribe [permission only]	Grants permission to unsubscribe from Amazon QuickSight, which permanently deletes all users and their resources from Amazon QuickSight	Write			
UntagResource	Grants permission to remove tags from a QuickSight resource	Tagging	actionconnector		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			emailCustomizationTemplate		
			flow		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAccountCustomPermission	Grants permission to update the custom permission associated with an account	Write			
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			
UpdateActionConnector	Grants permission to update an action connector	Write	actionconnector*		
UpdateActionConnectorPermissions	Grants permission to update permissions for an action connector	Permissions management	actionconnector*		
UpdateAgentPermissions [permission only]	Grants permission to update agent permissions	Permissions management	agent*		
UpdateAnalysis	Grants permission to update an analysis	Write	analysis*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
UpdateBrandPublishedVersion	Grants permission to update the published version of a brand	Write	brand*		
UpdateChatConfiguration [permission only]	Grants permission to update chat configuration	Write			
UpdateCustomPermissions	Grants permission to update a QuickSight custom permissions resource	Write	custompermissions*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateExtensionAccess [permission only]	Grants permission to update an extension access	Write	extensionaccess*		
UpdateFlowPermissions	Grants permission to update permissions for a flow	Permissions management	flow*		
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 AWS 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			
UpdateQuickIndexCapacity [permission only]	Grants permission to update index capacity	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateQuickSightQSearchConfiguration	Grants permission to update QuickSight Q Search configuration	Write			
UpdateRefreshSchedule	Grants permission to update a refresh schedule for a dataset	Write	refreshschedule*		
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			
UpdateSelfUpgrade	Grants permission to take action on pending self upgrade requests associated with an account	Write	user*		
UpdateSelfUpgradeConfiguration	Grants permission to update the administrative self upgrade configuration associated with an account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateThemePermissions	Grants permission to update permissions for a theme	Permissions management	theme*		
UpdateTopic	Grants permission to update a topic	Write	topic*		quicksight:PassDataSet
			dataset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}`	
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}

Resource types	ARN	Condition keys
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/${TagKey}
ingestion	arn:${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}

Resource types	ARN	Condition keys
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/${ResourceId}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}
brand	arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}	aws:ResourceTag/${TagKey}
custompermissions	arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}	aws:ResourceTag/${TagKey}
actionconnector	arn:${Partition}:quicksight:${Region}:${Account}:action-connector/${ResourceId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
agent	arn:${Partition}:quicksight:${Region}:${Account}:agent/${ResourceId}	
extension access	arn:${Partition}:quicksight:${Region}:${Account}:extension-access/${ResourceId}	
flow	arn:${Partition}:quicksight:${Region}:${Account}:flow/${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 AWS 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
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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddRoleToDBCluster	Grants permission to associate an Identity and Access Management (IAM) role from an Aurora DB cluster	Write	cluster*		iam:PassRole
AddRoleToDBInstance	Grants permission to associate an AWS Identity and Access Management (IAM) role with a DB instance	Write	db*		iam:PassRole
AddSourceIdentifierToSubscription	Grants permission to add a source identifier to an existing RDS event notification subscription	Write	es*		
AddTagsToResource	Grants permission to add metadata tags to an Amazon RDS resource	Tagging	auto-backup		
			cev		
			cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-auto-backup		
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		
			es		
			global-cluster		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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} rds:TagsFromRequest	
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/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CopyDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster-snapshot*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CopyDBParameterGroup	Grants permission to copy the specified DB parameter group	Write	pg*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyDBSnapshot	Grants permission to copy the specified DB snapshot	Write	snapshot*		rds:AddTagsToResource rds:CopyCustomDBEngineVersion
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} 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/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster		
			cluster-pg		
			db		
			pg		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rds:cluster-tag/${TagKey} rds:cluster-pg-tag/${TagKey} rds:db-tag/${TagKey} rds:pg-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:DatabaseClass rds:StorageSize rds:MultiAz rds:Piops rds:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomDBEngineVersion	Grants permission to create a custom engine version	Write	cev*		iam:CreateServiceLinkedRole mediaimport:CreateDatabaseBinarySnapshot rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBCluster	Grants permission to create a new DB cluster	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateDBInstance secretsmanager:CreateSecret secretsmanager:TagResource
			cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og*		
			subgrp*		
			db		
			global-cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:DatabaseClass rds:StorageSize rds:Piops rds:ManageMasterUs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				erPassword	
CreateDBClusterEndpoint	Grants permission to create a new custom endpoint and associates it with an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster*		rds:AddTagsToResource
			cluster-endpoint*		
				rds:EndpointType aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBClusterParameterGroup	Grants permission to create a new DB cluster parameter group	Write	cluster-pg*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster*		rds:AddTagsToResource
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBInstance	Grants permission to create a new DB instance	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateTenantDatabase secretsmanager:CreateSecret secretsmanager:TagResource
			cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og		
			pg		
			secgrp		
			subgrp		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBInstanceReadReplica	Grants permission to create a DB instance that acts as a Read Replica of a source DB instance	Write	cluster*		iam:PassRole rds:AddTagsToResource
			db*		
			og*		
			pg*		
			subgrp*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBParameterGroup	Grants permission to create a new DB parameter group	Write	pg*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBProxy	Grants permission to create a database proxy	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole rds:AddTagsToResource
CreateDBProxyEndpoint	Grants permission to create a database proxy endpoint	Write	proxy*		rds:AddTagsToResource
			proxy-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDBSecurityGroup	Grants permission to create a new DB security group. DB security groups control access to a DB instance	Write	secgrp*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBShardGroup	Grants permission to create a new Aurora Limitless Database DB shard group	Write	cluster*		rds:AddTagsToResource
			shardgrp*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:PubliclyAccessible	
CreateDBSnapshot	Grants permission to create a DBSnapshot	Write	db*		rds:AddTagsToResource
			snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBSubnetGroup	Grants permission to create a new DB subnet group	Write	subgrp*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventSubscription	Grants permission to create an RDS event notification subscription	Write	es*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateGlobalCluster	Grants permission to create an Aurora global database or DocumentDB global database spread across multiple regions	Write	cluster*		rds:AddTagsToResource
			global-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateIntegration	Grants permission to create an Aurora zero-ETL integration with Redshift	Write	cluster*		kms:CreateGrant kms:DescribeKey rds:AddTagsToResource
			integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateOptionGroup	Grants permission to create a new option group	Write	og*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateTenantDatabase	Grants permission to create a new tenant database	Write	db*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			tenant-database*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:TenantDatabaseName rds:ManageMasterUserPassword	
CrossRegionCommunication [permission only]	Grants permission to access a resource in the remote Region when executing cross-Region operations, such as cross-Region snapshot copy or cross-Region read replica creation	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBlueGreenDeployment	Grants permission to delete blue green deployments	Write	deployment*		rds:DeleteDBCluster rds:DeleteDBClusterEndpoint rds:DeleteDBInstance rds:PromoteReadReplica rds:PromoteReadReplicaDBCluster
				aws:ResourceTag/${TagKey}	
DeleteCustomDBEngineVersion	Grants permission to delete an existing custom engine version	Write	cev*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBCluster	Grants permission to delete a previously provisioned DB cluster	Write	cluster*		rds:AddTagsToResource rds:CreateDBClusterSnapshot rds:DeleteDBInstance
			cluster-snapshot*		
DeleteDBClusterAutomatedBackup	Grants permission to delete cluster automated backups based on the source cluster's DbClusterResourceId value or the restorable cluster's resource ID	Write	cluster-auto-backup*		
DeleteDBClusterEndpoint	Grants permission to delete a custom endpoint and removes it from an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster-endpoint*		
DeleteDBClusterParameterGroup	Grants permission to delete a specified DB cluster parameter group	Write	cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBClusterSnapshot	Grants permission to delete a DB cluster snapshot	Write	cluster-snapshot*		
DeleteDBInstance	Grants permission to delete a previously provisioned DB instance	Write	db*		rds:AddTagsToResource rds:CreateDBSnapshot rds:DeleteTenantDatabase
DeleteDBInstanceAutomatedBackup	Grants permission to delete automated backups based on the source instance's DbiResourceId value or the restorable instance's resource ID	Write	auto-backup*		
DeleteDBParameterGroup	Grants permission to delete a specified DBParameterGroup	Write	pg*		
DeleteDBProxy	Grants permission to delete a database proxy	Write	proxy*		
DeleteDBProxyEndpoint	Grants permission to delete a database proxy endpoint	Write	proxy-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBSecurityGroup	Grants permission to delete a DB security group	Write	secgrp*		
DeleteDBShardGroup	Grants permission to delete an Aurora Limitless Database DB shard group	Write	shardgrp*		
DeleteDBSnapshot	Grants permission to delete a DBSnapshot	Write	snapshot*		
DeleteDBSubnetGroup	Grants permission to delete a DB subnet group	Write	subgrp*		
DeleteEventSubscription	Grants permission to delete an RDS event notification subscription	Write	es*		
DeleteGlobalCluster	Grants permission to delete a global database cluster	Write	global-cluster*		
DeleteIntegration	Grants permission to delete an Aurora zero-ETL integration with Redshift	Write	integration*		
DeleteOptionGroup	Grants permission to delete an existing option group	Write	og*		
DeleteTenantDatabase	Grants permission to delete a tenant database	Write	db*		rds:AddTagsToResource rds:CreateDBSnapshot

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			tenant-database*		
DeregisterDBProxyTargets	Grants permission to remove targets from a database proxy target group	Write	cluster*		
			db*		
			proxy*		
			target-group*		
DescribeAccountAttributes	Grants permission to list all of the attributes for a customer account	List			
DescribeBlueGreenDeployments	Grants permission to describe blue green deployments	List	deployment		
DescribeCertificates	Grants permission to list the set of CA certificates provided by Amazon RDS for this AWS account	List			
DescribeDBClusterAutomatedBackups	Grants permission to return a list of cluster automated backups for both current and deleted clusters	List	cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBClusterBacktracks	Grants permission to return information about backtracks for a DB cluster	List	cluster*		
DescribeDBClusterEndpoints	Grants permission to return information about endpoints for an Amazon Aurora DB cluster	List	cluster		
			cluster-endpoint		
DescribeDBClusterParameterGroups	Grants permission to return a list of DBClusterParameter Group descriptions	List	cluster-pg		
DescribeDBClusterParameters	Grants permission to return the detailed parameter list for a particular DB cluster parameter group	List	cluster-pg*		
DescribeDBClusterSnapshotAttributes	Grants permission to return a list of DB cluster snapshot attribute names and values for a manual DB cluster snapshot	List	cluster-snapshot*		
DescribeDBClusterSnapshots	Grants permission to return information about DB cluster snapshots	List	cluster		
			cluster-snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBClusters	Grants permission to return information about provisioned Aurora DB clusters or DocumentDB clusters	List	cluster		
DescribeDBEngineVersions	Grants permission to return a list of the available DB engines	List			
DescribeDBInstanceAutomatedBackups	Grants permission to return a list of automated backups for both current and deleted instances	List	auto-backup		
			db		
DescribeDBInstances	Grants permission to return information about provisioned RDS instances	List	db		
DescribeDBLogFiles	Grants permission to return a list of DB log files for the DB instance	List	db*		
DescribeDBMajorEngineVersions	Grants permission to return information specific for each DB major engine versions	List			
DescribeDBParameterGroups	Grants permission to return a list of DBParameterGroup descriptions	List	pg		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBParameters	Grants permission to return the detailed parameter list for a particular DB parameter group	List	pg*		
DescribeDBProxies	Grants permission to view proxies	List	proxy		
DescribeDBProxyEndpoints	Grants permission to view proxy endpoints	List	proxy		
			proxy-endpoint		
DescribeDBProxyTargetGroups	Grants permission to view database proxy target group details	List	proxy*		
DescribeDBProxyTargets	Grants permission to view database proxy target details	List	proxy*		
			target-group*		
DescribeDBRecommendations	Grants permission to list recommendation details	List			
DescribeDBSecurityGroups	Grants permission to return a list of DBSecurityGroup descriptions	List	secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBShardGroups	Grants permission to return information about all Aurora Limitless Database DB shard groups for this account. You can filter by shard group(s)	List	shardgrp		
DescribeDBSnapshotAttributes	Grants permission to return a list of DB snapshot attribute names and values for a manual DB snapshot	List	snapshot*		
DescribeDBSnapshotTenantDatabases	Grants permission to return information about tenant databases in DB snapshots. You can filter by Region or snapshot	List	db		
			snapshot		
			snapshot-tenant-database		
DescribeDBSnapshots	Grants permission to return information about DB snapshots	List	db		
			snapshot		
DescribeDBSubnetGroups	Grants permission to return a list of DBSubnetGroup descriptions	List	subgrp		
DescribeEngineDefaultClusterParameters	Grants permission to return the default engine and system parameter information for the cluster database engine	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEngineDefaultParameters	Grants permission to return the default engine and system parameter information for the specified database engine	List			
DescribeEventCategories	Grants permission to display a list of categories for all event source types, or, if specified, for a specified source type	List			
DescribeEventSubscriptions	Grants permission to list all the subscription descriptions for a customer account	List	es		
DescribeEvents	Grants permission to return events related to DB instances, DB security groups, DB snapshots, and DB parameter groups for the past 14 days	List			
DescribeExportTasks	Grants permission to return information about the export tasks	List	cluster		
			cluster-snapshot		
			snapshot		
DescribeGlobalClusters	Grants permission to return information about Aurora global database clusters or DocumentDB global database clusters	List	global-cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIntegrations	Grants permission to describe an Aurora zero-ETL integration with Redshift	List	integration		
				aws:ResourceTag/${TagKey}	
DescribeOptionGroupOptions	Grants permission to describe all available options	List			
DescribeOptionGroups	Grants permission to describe the available option groups	List	og		
DescribeOrderableDBInstanceOptions	Grants permission to return a list of orderable DB instance options for the specified engine	List			
DescribePendingMaintenanceActions	Grants permission to return a list of resources (for example, DB instances) that have at least one pending maintenance action	List	cluster		
			db		
DescribeRecommendationGroups [permission only]	Grants permission to return information about recommendation groups	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRecommendations [permission only]	Grants permission to return information about recommendations	Read			
DescribeReservedDBInstances	Grants permission to return information about reserved DB instances for this account, or about a specified reserved DB instance	List	ri		
DescribeReservedDBInstancesOfferings	Grants permission to list available reserved DB instance offerings	List			
DescribeSourceRegions	Grants permission to return a list of the source AWS Regions where the current AWS Region can create a Read Replica or copy a DB snapshot from	List			
DescribeTenantDatabases	Grants permission to return information about provisioned tenant databases. You can filter by Region or snapshot	List	db tenant-database		
DescribeValidDBInstanceModifications	Grants permission to list available modifications you can make to your DB instance	List	db*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableHttpEndpoint	Grants permission to disable http endpoint for a DB cluster	Write	cluster*		
DownloadCompleteDBLogFile	Grants permission to download specified log file	Read	db*		
DownloadDBLogFilePortion	Grants permission to download all or a portion of the specified log file, up to 1 MB in size	Read	db*		
EnableHttpEndpoint	Grants permission to enable http endpoint for a DB cluster	Write	cluster*		
FailoverDBCluster	Grants permission to force a failover for a DB cluster	Write	cluster*		
FailoverGlobalCluster	Grants permission to failover a global cluster	Write	cluster*		
			global-cluster*		
ListTagsForResource	Grants permission to list all tags on an Amazon RDS resource	Read	auto-backup		
			cev		
			cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			es		
			global-cluster		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			shardgrp		
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
ModifyActivityStream	Grants permission to modify a database activity stream	Write	db*		
ModifyCertificates	Grants permission to modify the system-default Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificate for Amazon RDS for new DB instances	Write			
ModifyCurrentDBClusterCapacity	Grants permission to modify current cluster capacity for an Amazon Aurora Serverless DB cluster	Write	cluster*		
ModifyCustomDBEngineVersion	Grants permission to modify an existing custom engine version	Write	cev*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyDBCluster	Grants permission to modify a setting for an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:ModifyDBInstance secretsmanager:CreateSecret secretsmanager:RotateSecret secretsmanager:TagResource
			cluster-pg		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og		
			pg		
				rds:DatabaseClass rds:StorageSize rds:Piops rds:ManageMasterUserPassword	
ModifyDBClusterEndpoint	Grants permission to modify the properties of an endpoint in an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster-endpoint*		
ModifyDBClusterParameterGroup	Grants permission to modify the parameters of a DB cluster parameter group	Write	cluster-pg*		
ModifyDBClusterSnapshotAttribute	Grants permission to add an attribute and values to, or removes an attribute and values from, a manual DB cluster snapshot	Write	cluster-snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyDBInstance	Grants permission to modify settings for a DB instance	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateTenantDatabase secretsmanager:CreateSecret secretsmanager:RotateSecret

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:TagResource
			og		
			pg		
			secgrp		
			subgrp		
				rds:ManageMasterUserPassword	
ModifyDBParameterGroup	Grants permission to modify the parameters of a DB parameter group	Write	pg*		
ModifyDBProxy	Grants permission to modify database proxy	Write	proxy*		iam:PassRole
ModifyDBProxyEndpoint	Grants permission to modify database proxy endpoint	Write	proxy-endpoint*		
ModifyDBProxyTargetGroup	Grants permission to modify target group for a database proxy	Write	target-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyDBRecommendation	Grants permission to modify recommendation	Write			
ModifyDBShardGroup	Grants permission to modify properties of an Aurora Limitless Database DB shard group	Write	shardgrp*		
ModifyDBSnapshot	Grants permission to update a manual DB snapshot, which can be encrypted or not encrypted, with a new engine version	Write	snapshot* og		
ModifyDBSnapshotAttribute	Grants permission to add an attribute and values to, or removes an attribute and values from, a manual DB snapshot	Write	snapshot*		
ModifyDBSubnetGroup	Grants permission to modify an existing DB subnet group	Write	subgrp*		
ModifyEventSubscription	Grants permission to modify an existing RDS event notification subscription	Write	es*		
ModifyGlobalCluster	Grants permission to modify a setting for an Amazon Aurora global cluster or Amazon DocumentDB global cluster	Write	global-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIntegration	Grants permission to modify an Aurora zero-ETL integration with Redshift	Write	integration*		
ModifyOptionGroup	Grants permission to modify an existing option group	Write	og*		iam:PassRole
ModifyRecommendation [permission only]	Grants permission to modify recommendation	Write			
ModifyTenantDatabase	Grants permission to modify a tenant database	Write	db*		
			tenant-database*		
				rds:TenantDatabaseName rds:ManageMasterUserPassword	
PromoteReadReplica	Grants permission to promote a Read Replica DB instance to a standalone DB instance	Write	db*		rds:AddTagsToResource
PromoteReadReplicaDBCluster	Grants permission to promote a Read Replica DB cluster to a standalone DB cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseReservedDBInstancesOffering	Grants permission to purchase a reserved DB instance offering	Write	ri*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
RebootDBCluster	Grants permission to reboot a previously provisioned DB cluster	Write	cluster*		rds:RebootDBInstance
RebootDBInstance	Grants permission to restart the database engine service	Write	db*		
RebootDBShardGroup	Grants permission to reboot an Aurora Limitless Database DB shard group	Write	shardgrp*		
RegisterDBProxyTargets	Grants permission to add targets to a database proxy target group	Write	target-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveFromGlobalCluster	Grants permission to detach an Aurora secondary cluster from an Aurora global database cluster or DocumentDB global cluster	Write	cluster*		
			global-cluster*		
RemoveRoleFromDBCluster	Grants permission to disassociate an AWS Identity and Access Management (IAM) role from an Amazon Aurora DB cluster	Write	cluster*		iam:PassRole
RemoveRoleFromDBInstance	Grants permission to disassociate an AWS Identity and Access Management (IAM) role from a DB instance	Write	db*		iam:PassRole
RemoveSourceIdentifierFromSubscription	Grants permission to remove a source identifier from an existing RDS event notification subscription	Write	es*		
RemoveTagsFromResource	Grants permission to remove metadata tags from an Amazon RDS resource	Tagging	auto-backup		
			cev		
			cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		
			es		
			global-cluster		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			shardgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
ResetDBClusterParameterGroup	Grants permission to modify the parameters of a DB cluster parameter group to the default value	Write	cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetDBParameterGroup	Grants permission to modify the parameters of a DB parameter group to the engine/system default value	Write	pg*		
RestoreDBClusterFromS3	Grants permission to create an Amazon Aurora DB cluster from data stored in an Amazon S3 bucket	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource secretsmanager:CreateSecret secretsmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-pg*		
			og*		
			subgrp*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:ManageMasterUserPassword	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreDBClusterFromSnapshot	Grants permission to create a new DB cluster from a DB cluster snapshot	Write	cluster*		iam:PassRole rds:AddTagsToResource rds:CreateDBInstance
			cluster-pg*		
			og*		
			subgrp*		
			cluster-snapshot		
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseClass rds:StorageSize rds:Piops	
RestoreDBClusterToPointInTime	Grants permission to restore a DB cluster to an arbitrary point in time	Write	cluster*		iam:PassRole rds:AddTagsToResource rds:CreateDBInstance
			cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og*		
			subgrp*		
			cluster-auto-backup		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseClass rds:StorageSize rds:Piops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreDBInstanceFromDBSnapshot	Grants permission to create a new DB instance from a DB snapshot	Write	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		
			pg*		
			subgrp*		
			cluster-snapshot		
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreDBInstanceFromS3	Grants permission to create a new DB instance from an Amazon S3 bucket	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource secretsmanager:CreateSecret secretsmanager:TagResource
			og*		
			pg*		
			subgrp*		
			secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	
RestoreDBInstanceToPointInTime	Grants permission to restore a DB instance to an arbitrary point in time	Write	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			pg*		
			subgrp*		
			auto-backup		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeDBSecurityGroupIngress	Grants permission to revoke ingress from a DBSecurityGroup for previously authorized IP ranges or EC2 or VPC Security Groups	Write	secgrp*		
StartActivityStream	Grants permission to start Activity Stream	Write	cluster		
			db		
StartDBCluster	Grants permission to start the DB cluster	Write	cluster*		
StartDBInstance	Grants permission to start the DB instance	Write	db*		
StartDBInstanceAutomatedBackupsReplication	Grants permission to start replication of automated backups to a different AWS Region	Write	auto-backup*		rds:AddTagsToResource
			db*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartExportTask	Grants permission to start a new Export task for a DB snapshot	Write	cluster		iam:PassRole
			cluster-snapshot		
			snapshot		
StopActivityStream	Grants permission to stop Activity Stream	Write	cluster		
			db		
StopDBCluster	Grants permission to stop the DB cluster	Write	cluster*		
StopDBInstance	Grants permission to stop the DB instance	Write	db*		rds:AddTagsToResource rds:CreateDBSnapshot
			snapshot		
StopDBInstanceAutomatedBackupsReplication	Grants permission to stop automated backup replication for a DB instance	Write	db*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SwitchoverBlueGreenDeployment	Grants permission to switch a blue-green deployment from source instance or cluster to target	Write	deployment*		rds:ModifyDBCluster rds:ModifyDBInstance rds:PromoteReadReplica rds:PromoteReadReplicaDBCluster
				aws:ResourceTag/${TagKey}	
SwitchoverGlobalCluster	Grants permission to switchover a global cluster	Write	cluster*		
			global-cluster*		
SwitchoverReadReplica	Grants permission to switch over a read replica, making it the new primary database	Write	db*		

Resource types defined by Amazon RDS

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} rds:cluster-tag/${TagKey}
shardgrp	`arn:${Partition}:rds:${Region}:${Account}:shard-group:${DbShardGroupResourceId}`	aws:ResourceTag/${TagKey}
cluster-auto-backup	`arn:${Partition}:rds:${Region}:${Account}:cluster-auto-backup:${DbClusterAutomatedBackupId}`	aws:ResourceTag/${TagKey}
auto-backup	`arn:${Partition}:rds:${Region}:${Account}:auto-backup:${DbInstanceAutomatedBackupId}`	aws:ResourceTag/${TagKey}
cluster-endpoint	`arn:${Partition}:rds:${Region}:${Account}:cluster-endpoint:${DbClusterEndpoint}`	aws:ResourceTag/${TagKey}
cluster-pg	`arn:${Partition}:rds:${Region}:${Account}:cluster-pg:${ClusterParameterGroupName}`	aws:ResourceTag/${TagKey} rds:cluster-pg-tag/${TagKey}

Resource types	ARN	Condition keys
cluster-snapshot	arn:${Partition}:rds:${Region}:${Account}:cluster-snapshot:${ClusterSnapshotName}	aws:ResourceTag/${TagKey} rds:cluster-snapshot-tag/${TagKey}
db	arn:${Partition}:rds:${Region}:${Account}:db:${DbInstanceName}	aws:ResourceTag/${TagKey} rds:DatabaseClass rds:DatabaseEngine rds:DatabaseName rds:MultiAz rds:Piops rds:StorageEncrypted rds:StorageSize rds:Vpc rds:db-tag/${TagKey}
es	arn:${Partition}:rds:${Region}:${Account}:es:${SubscriptionName}	aws:ResourceTag/${TagKey} rds:es-tag/${TagKey}
global-cluster	arn:${Partition}:rds::${Account}:global-cluster:${GlobalCluster}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
og	arn:${Partition}:rds:${Region}:${Account}:og:${OptionGroupName}	aws:ResourceTag/${TagKey} rds:og-tag/${TagKey}
pg	arn:${Partition}:rds:${Region}:${Account}:pg:${ParameterGroupName}	aws:ResourceTag/${TagKey} rds:pg-tag/${TagKey}
proxy	arn:${Partition}:rds:${Region}:${Account}:db-proxy:${DbProxyId}	aws:ResourceTag/${TagKey}
proxy-endpoint	arn:${Partition}:rds:${Region}:${Account}:db-proxy-endpoint:${DbProxyEndpointId}	aws:ResourceTag/${TagKey}
ri	arn:${Partition}:rds:${Region}:${Account}:ri:${ReservedDbInstanceName}	aws:ResourceTag/${TagKey} rds:ri-tag/${TagKey}
secgrp	arn:${Partition}:rds:${Region}:${Account}:secgrp:${SecurityGroupName}	aws:ResourceTag/${TagKey} rds:secgrp-tag/${TagKey}
snapshot	arn:${Partition}:rds:${Region}:${Account}:snapshot:${SnapshotName}	aws:ResourceTag/${TagKey} rds:snapshot-tag/${TagKey}

Resource types	ARN	Condition keys
subgrp	arn:${Partition}:rds:${Region}:${Account}:subgrp:${SubnetGroupName}	aws:ResourceTag/${TagKey} rds:subgrp-tag/${TagKey}
target-group	arn:${Partition}:rds:${Region}:${Account}:target-group:${TargetGroupId}	aws:ResourceTag/${TagKey}
cev	arn:${Partition}:rds:${Region}:${Account}:cev:${Engine}/${EngineVersion}/${CustomDbEngineVersionId}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:rds:${Region}:${Account}:deployment:${BlueGreenDeploymentIdentifier}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:rds:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}
snapshot-tenant-database	arn:${Partition}:rds:${Region}:${Account}:snapshot-tenant-database:${SnapshotName}:${TenantResourceId}	aws:ResourceTag/${TagKey}
tenant-database	arn:${Partition}:rds:${Region}:${Account}:tenant-database:${TenantResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon RDS

Amazon RDS defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the set of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the set of tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the set of tag keys in the request	ArrayOfString
rds:BackupTarget	Filters access by the type of backup target. One of: region, outposts	String
rds:CopyOptionGroup	Filters access by the value that specifies whether the CopyDBSnapshot action requires copying the DB option group	Bool
rds:DatabaseClass	Filters access by the type of DB instance class	String
rds:DatabaseEngine	Filters access by the database engine. For possible values refer to the engine parameter in CreateDBInstance API	String
rds:DatabaseName	Filters access by the user-defined name of the database on the DB instance	String
rds:EndpointType	Filters access by the type of the endpoint. One of: READER, WRITER, CUSTOM	String
rds:ManageMasterUserPassword	Filters access by the value that specifies whether RDS manages master user password in AWS Secrets Manager for the DB instance or cluster	Bool

Condition keys	Description	Type
rds:MultiAz	Filters access by the value that specifies whether the DB instance runs in multiple Availability Zones. To indicate that the DB instance is using Multi-AZ, specify true	Bool
rds:Piops	Filters access by the value that contains the number of Provisioned IOPS (PIOPS) that the instance supports. To indicate a DB instance that does not have PIOPS enabled, specify 0	Numeric
rds:PubliclyAccessible	Filters access by the value that specifies whether the DB Instance or DB ShardGroup is publicly accessible	Bool
rds:StorageEncrypted	Filters access by the value that specifies whether the DB instance storage should be encrypted. To enforce storage encryption, specify true	Bool
rds:StorageSize	Filters access by the storage volume size (in GB)	Numeric
rds:TagsFromRequest	Filters access for rds:AddTagsToResource based on whether tags are explicitly specified in the Tags or TagSpecification request parameters. Evaluates to true when tags are provided in these parameters. Evaluates as false when tags are implicitly inherited from source resources	Bool
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

Condition keys	Description	Type
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
rds:db-tag/${TagKey}	Filters access by the tag attached to a DB instance	String
rds:es-tag/${TagKey}	Filters access by the tag attached to an event subscription	String
rds:og-tag/${TagKey}	Filters access by the tag attached to a DB option group	String
rds:pg-tag/${TagKey}	Filters access by the tag attached to a DB parameter group	String
rds:req-tag/${TagKey}	Filters access by the set of tag keys and values that can be used to tag a resource	String
rds:ri-tag/${TagKey}	Filters access by the tag attached to a reserved DB instance	String
rds:secgrp-tag/${TagKey}	Filters access by the tag attached to a DB security group	String
rds:snapshot-tag/${TagKey}	Filters access by the tag attached to a DB snapshot	String
rds:subgrp-tag/${TagKey}	Filters access by the tag attached to a DB subnet group	String

Actions, resources, and condition keys for Amazon RDS Data API

Amazon RDS Data API (service prefix: `rds-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 RDS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchExecuteStatement	Grants permission to run a batch SQL statement over an array of data	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BeginTransaction	Grants permission to start a SQL transaction	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
CommitTransaction	Grants permission to end a SQL transaction started with the BeginTransaction operation and commits the changes	Write	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteSql	Grants permission to run one or more SQL statements. This operation is deprecated. Use the BatchExecuteStatement or ExecuteStatement operation	Write	cluster*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ExecuteStatement		Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to run a SQL statement against a database			aws:ResourceTag/${TagKey} aws:TagKeys	
RollbackTransaction	Grants permission to perform a rollback of a transaction. Rolling back a transaction cancels its changes	Write	cluster*		rds-data:BeginTransaction
				aws:ResourceTag/${TagKey} aws:TagKeys	

Resource types defined by Amazon RDS 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:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}	aws:ResourceTag/${TagKey} aws:TagKeys

Condition keys for Amazon RDS Data API

Amazon RDS 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 AWS global condition context keys.

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 associated with the resource	ArrayOfString

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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Recycle Bin

AWS 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 AWS Recycle Bin
- Resource types defined by AWS Recycle Bin
- Condition keys for AWS Recycle Bin

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRule	Grants permission to create a Recycle Bin retention rule	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/ResourceType	
DeleteRule	Grants permission to delete a Recycle Bin retention rule	Write	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	Grants permission to get detailed information about a Recycle Bin retention rule	Read	rule*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rbin:Attribute/ResourceType	
ListRules	Grants permission to list the Recycle Bin retention rules in the Region	Read		rbin:Request/ResourceType	
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	rule*		
				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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add or update tags of a resource	Tagging	rule*		
				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		Tagging	rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to remove tags associated with a resource			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 AWS 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 AWS Recycle Bin

AWS 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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 *		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				redshift:ConsumerArn 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 AWS 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/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Grants permission to create an Amazon Redshift parameter group	Write	parametergroup*		
				aws:RequestTag/${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			
CreateSnapshotCopyGrant	Grants permission to create a snapshot copy grant and encrypt copied snapshots in a destination AWS Region	Permissions management	snapshotcopygrant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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		
			integration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			parameter group		
			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 AWS account	Read			
DescribeAuthenticationProfiles	Grants permission to describe created Amazon Redshift authentication profiles	Read			
DescribeAutonomicsDenylist [permission only]	Grants permission to describe the list of resources that are denylisted from global autonomics decisions for a specified cluster	Read	cluster*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClusterSnapshots	Grants permission to describe one or more snapshot objects, which contain metadata about your cluster snapshots	Read			
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	cluster		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDataSharesForConsumer	Grants permission to describe only datashares consumed by your clusters	Read			
DescribeDataSharesForProducer	Grants permission to describe only datashares created by your clusters	Read			
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 AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEvents	Grants permission to describe events related to clusters, security groups, snapshots, and parameter groups for the past 14 days	List			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRedshiftIdcApplications	Grants permission to describe redshift idc applications	List			sso:GetApplicationGrant sso:ListApplicationAccessScopes
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScheduledActions	Grants permission to describe created Amazon Redshift scheduled actions	Read			
DescribeSnapshotCopyGrants	Grants permission to describe snapshot copy grants owned by the specified AWS account in the destination AWS 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 AWS account	Write	dbuser*		
			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 AWS account	Write	dbname		
				redshift:DbName redshift:DurationSeconds	
GetIdentityCenterAuthToken	Grants permission to get an authorized token for Identity Center users to access Redshift clusters	Read	cluster*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
JoinGroup	Grants permission to join the specified Amazon Redshift group	Permissions management	dbgroup*		
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
ModifyAutonomicsDenylist [permission only]	Grants permission to add or remove resources from the global autonomics denylist for a specified cluster	Write	cluster*		

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 AWS Identity and Access Management (IAM) roles that can be used by a cluster to access other AWS services	Permissions management	cluster*		
ModifyClusterMaintenance	Grants permission to modify the maintenance settings of a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyClusterParameterGroup	Grants permission to modify the parameters of a parameter group	Write	parameter group*		
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 AWS Region after they are copied from the source AWS 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	parametergroup*		
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 AWS 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:${ClusterNamespace}	
parametergroup	arn:${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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchExecuteStatement	Grants permission to execute multiple queries under a single connection	Write	cluster		
			workgroup		
				redshift-data:session-owner-iam-userid	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				redshift-data:glue-catalog-arn	
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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConvertRecoveryPointToSnapshot	Grants permission to convert a recovery point to a snapshot	Write	recoveryPoint*		
			snapshot*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateCustomDomainAssociation	Grants permission to create a custom domain association in Amazon Redshift Serverless	Write	workgroup*		acm:DescribeCertificate
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	namespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot*		
				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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomDomainAssociation	Grants permission to delete a custom domain association	Write	workgroup*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSnapshotCopyConfiguration	Grants permission to delete a snapshot copy configuration for a Amazon Redshift Serverless namespace	Write			
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
GetIdentityCenterAuthToken	Grants permission to get an authorized token for Identity Center users to access Redshift Serverless workgroups	Read	workgroup*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSnapshot	Grants permission to get information about a specific snapshot	Read	snapshot*		
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*		
ListAutonomicsDenylist [permission only]	Grants permission to list the resources that are denylisted from global autonomics decisions for a specified workgroup	Read	workgroup*		
ListCustomDomainAssociations	Grants permission to list custom domain associations in Amazon Redshift Serverless	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListRecoveryPoints	Grants permission to list an array of recovery points	List	recoveryPoint*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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	
UpdateAutonomicsDenylist [permission only]	Grants permission to add or remove resources from the global autonomics denylist for a specified workgroup	Write	workgroup *		
UpdateCustomDomainAssociation	Grants permission to update a certificate associated with a custom domain	Write	workgroup *		acm:DescribeCertificate

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
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 Rekognition

Amazon Rekognition (service prefix: `rekognition`) 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 Rekognition
- Resource types defined by Amazon Rekognition
- Condition keys for Amazon Rekognition

Actions defined by Amazon Rekognition

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFaces	Grants permission to associate multiple individual faces with a single user	Write	collection*		
CompareFaces	Grants permission to compare faces in the source input image with each face detected in the target input image	Read			
CopyProjectVersion	Grants permission to copy an existing model version to a new model version	Write	project*		
			projectversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCollection	Grants permission to create a collection in an AWS Region	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateDataset	Grants permission to create a new Amazon Rekognition Custom Labels dataset	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFaceLivenessSession	Grants permission to create a face liveness session	Write			
CreateProject	Grants permission to create an Amazon Rekognition Custom Labels project	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProjectVersion	Grants permission to begin training a new version of a model	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStreamProcessor	Grants permission to create an Amazon Rekognition stream processor	Write	collection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Grants permission to create a new user in a collection using a unique user ID you provide	Write	collection*		
DeleteCollection	Grants permission to delete the specified collection	Write	collection*		
DeleteDataset	Grants permission to delete an existing Amazon Rekognition Custom Labels dataset	Write	dataset*		
DeleteFaces	Grants permission to delete faces from a collection	Write	collection*		
DeleteProject	Grants permission to delete a project	Write	project*		
DeleteProjectPolicy	Grants permission to delete a resource policy attached to a project	Write	project*		
DeleteProjectVersion	Grants permission to delete a model	Write	projectversion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStreamProcessor	Grants permission to delete the specified stream processor	Write	streamprocessor*		
DeleteUser	Grants permission to delete a user from a collection based on the provided user ID	Write	collection*		
DescribeCollection	Grants permission to read details about a collection	Read	collection*		
DescribeDataset	Grants permission to describe an Amazon Rekognition Custom Labels dataset	Read	dataset*		
DescribeProjectVersions	Grants permission to list the versions of a model in an Amazon Rekognition Custom Labels project	Read	project*		
DescribeProjects	Grants permission to list Amazon Rekognition Custom Labels projects	Read			
DescribeStreamProcessor	Grants permission to get information about the specified stream processor	Read	streamprocessor*		
DetectCustomLabels	Grants permission to detect custom labels in a supplied image	Read	projectversion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetectFaces	Grants permission to detect human faces within an image provided as input	Read			
DetectLabels	Grants permission to detect instances of real-world labels within an image provided as input	Read			
DetectModerationLabels	Grants permission to detect moderation labels within the input image	Read	projectversion		
DetectProtectiveEquipment	Grants permission to detect Personal Protective Equipment in the input image	Read			
DetectText	Grants permission to detect text in the input image and convert it into machine-readable text	Read			
DisassociateFaces	Grants permission to remove the association between a user ID and a face ID	Write	collection*		
DistributeDatasetEntries	Grants permission to distribute the entries in a training dataset across the training dataset and the test dataset for a project	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCelebrityInfo	Grants permission to read the name, and additional information, of a celebrity	Read			
GetCelebrityRecognition	Grants permission to read the celebrity recognition results found in a stored video by an asynchronous celebrity recognition job	Read			
GetContentModeration	Grants permission to read the content moderation analysis results found in a stored video by an asynchronous content moderation job	Read			
GetFaceDetection	Grants permission to read the faces detection results found in a stored video by an asynchronous face detection job	Read			
GetFaceLivenessSessionResults	Grants permission to get results of a face liveness session	Read			
GetFaceSearch	Grants permission to read the matching collection faces found in a stored video by an asynchronous face search job	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLabelDetection	Grants permission to read the label detected resuls found in a stored video by an asynchronous label detection job	Read			
GetMediaAnalysisJob	Grants permission to read the reference to job results in S3 and additional information about a media analysis job	Read			
GetPersonTracking	Grants permission to read the list of persons detected in a stored video by an asynchronous person tracking job	Read			
GetSegmentDetection	Grants permission to get the vdeo segments found in a stored video by an asynchronous segment detection job	Read			
GetTextDetection	Grants permission to get the text found in a stored video by an asynchronous text detection job	Read			
IndexFaces	Grants permission to update an existing collection with faces detected in the input image	Write	collection*		
ListCollections	Grants permission to read the collection Id's in your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatasetEntries	Grants permission to list the dataset entries in an existing Amazon Rekognition Custom Labels dataset	Read	dataset*		
ListDatasetLabels	Grants permission to list the labels in a dataset	Read	dataset*		
ListFaces	Grants permission to read metadata for faces in the specificed collection	Read	collection*		
ListMediaAnalysisJobs	Grants permission to read the list of media analysis jobs	Read			
ListProjectPolicies	Grants permission to list the resource policies attached to a project	Read	project*		
ListStreamProcessors	Grants permission to get a list of your stream processors	List			
ListTagsForResource	Grants permission to return a list of tags associated with a resource	Read	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListUsers	Grants permission to list UserIds and the UserStatus	Read	collection*		
PutProjectPolicy	Grants permission to attach a resource policy to a project	Write	project*		
RecognizeCelebrities	Grants permission to detect celebrities in the input image	Read			
SearchFaces	Grants permission to search the specificed collection for the supplied face ID	Read	collection*		
SearchFacesByImage	Grants permission to search the specificed collection for the largest face in the input image	Read	collection*		
SearchUsers	Grants permission to search the specificed collection for user match result with given either face ID or user ID	Read	collection*		
SearchUsersByImage	Grants permission to search the specificed collection for user match result by using the largest face in the input image	Read	collection*		
StartCelebrityRecognition	Grants permission to start the asynchronous recognition of celebrities in a stored video	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartContentModeration	Grants permission to start asynchronous detection of explicit or suggestive adult content in a stored video	Write			
StartFaceDetection	Grants permission to start asynchronous detection of faces in a stored video	Write			
StartFaceLivenessSession	Grants permission to start streaming video for a face liveness session	Write			
StartFaceSearch	Grants permission to start an asynchronous search for faces in a collection that match the faces of persons detected in a stored video	Write	collection*		
StartLabelDetection	Grants permission to start asynchronous detection of labels in a stored video	Write			
StartMediaAnalysisJob	Grants permission to start a media analysis job	Write	projectversion		
StartPersonTracking	Grants permission to start the asynchronous tracking of persons in a stored video	Write			
StartProjectVersion	Grants permission to start running a model version	Write	projectversion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSegmentDetection	Grants permission to start the asynchronous detection of segments in a stored video	Write			
StartStreamProcessor	Grants permission to start running a stream processor	Write	streamprocessor*		
StartTextDetection	Grants permission to start the asynchronous detection of text in a stored video	Write			
StopProjectVersion	Grants permission to stop a running model version	Write	projectversion*		
StopStreamProcessor	Grants permission to stop a running stream processor	Write	streamprocessor*		
TagResource	Grants permission to add one or more tags to a resource	Tagging	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	collection		
			dataset		
			project		
			projectversion		
			streamprocessor		
				aws:TagKeys	
UpdateDatasetEntries	Grants permission to add or update one or more JSON Lines (entries) in a dataset	Write	dataset*		
UpdateStreamProcessor	Grants permission to modify properties for a stream processor	Write	streamprocessor*		

Resource types defined by Amazon Rekognition

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
collection	`arn:${Partition}:rekognition:${Region}:${Account}:collection/${CollectionId}`	aws:ResourceTag/${TagKey}
streamprocessor	`arn:${Partition}:rekognition:${Region}:${Account}:streamprocessor/${StreamprocessorId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}
projectversion	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/version/${VersionName}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}
dataset	`arn:${Partition}:rekognition:${Region}:${Account}:project/${ProjectName}/dataset/${DatasetType}/${CreationTimestamp}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Rekognition

Amazon Rekognition defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the

policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS rePost Private

AWS rePost Private (service prefix: `repostspace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS rePost Private
- Resource types defined by AWS rePost Private
- Condition keys for AWS rePost Private

Actions defined by AWS rePost Private

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAddChannelRoleToAccessors	Grants permission to add a role to users and groups in a private re:Post channel in your account	Write	space*		
BatchAddRole	Grants permission to add a role to users and groups in a private re:Post in your account	Write	space*		
BatchRemoveChannelRoleFromAccessors	Grants permission to remove a role from users and groups in a private re:Post channel in your account	Write	space*		
BatchRemoveRole	Grants permission to remove a role from users and groups in a private re:Post in your account	Write	space*		
CreateChannel	Grants permission to create a new channel in private re:Post in your account	Write	space*		
CreateSpace	Grants permission to create a new private re:Post in your account	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSpace	Grants permission to delete a private re:Post from your account	Write	space*		
DeregisterAdmin	Grants permission to remove an administrator to a private re:Post in your account	Write	space*		
GetChannel	Grants permission to get the description for a channel in private re:Post in your account	Read	space*		
GetSpace	Grants permission to get the description for a private re:Post in your account	Read	space*		
ListChannels	Grants permission to list all channels in a private re:Post in your account	Read	space*		
ListSpaces	Grants permission to list all private re:Posts in your account	Read			
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterAdmin	Grants permission to add an administrator to a private re:Post in your account	Write	space*		
SendInvites	Grants permission to send invites to users of a private re:Post in your account	Write	space*		
TagResource	Grants permission to tag a resource	Tagging	space*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	space*		
				aws:TagKeys	
UpdateChannel	Grants permission to update a channel in private re:Post in your account	Write	space*		
UpdateSpace	Grants permission to update a private re:Post in your account	Write	space*		

Resource types defined by AWS rePost Private

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
space	`arn:${Partition}:repostspace:${Region}:${Account}:space/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS rePost Private

AWS rePost Private defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Resilience Hub

AWS Resilience Hub (service prefix: `resiliencehub`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Resilience Hub

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptResourceGroupingRecommendations	Grants permission to accept resource grouping recommendations	Write	application*		
AddDraftAppVersionResourceMappings	Grants permission to add draft application version resource mappings	Write	application*		cloudformation:DescribeStacks

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
BatchUpdateRecommendationStatus	Grants permission to include or exclude one or more operational recommendations	Write	application*		
CreateApp	Grants permission to create application	Write	application*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAppVersionAppComponent	Grants permission to create application app component	Write	application*		
CreateAppVersionResource	Grants permission to create application resource	Write	application*		
CreateRecommendationTemplate	Grants permission to create recommendation template	Write	application*		s3:CreateBucket s3:ListBucket s3:PutObject
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResiliencyPolicy	Grants permission to create resiliency policy	Write	resiliency-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApp	Grants permission to batch delete application	Write	application*		
DeleteAppAssessment	Grants permission to batch delete application assessment	Write	application*		
DeleteAppInputSource	Grants permission to remove application input source	Write	application*		
DeleteAppVersionAppComponent	Grants permission to delete application app component	Write	application*		
DeleteAppVersionResource	Grants permission to delete application resource	Write	application*		
DeleteRecommendationTemplate	Grants permission to batch delete recommendation template	Write	application*		
DeleteResiliencyPolicy	Grants permission to batch delete resiliency policy	Write	resiliency-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeApp	Grants permission to describe application	Read	application*		
DescribeAppAssessment	Grants permission to describe application assessment	Read	application*		
DescribeAppVersion	Grants permission to describe application version	Read	application*		
DescribeAppVersionAppComponent	Grants permission to describe application version app component	Read	application*		
DescribeAppVersionResource	Grants permission to describe application version resource	Read	application*		
DescribeAppVersionResourcesResolutionStatus	Grants permission to describe application resolution	Read	application*		
DescribeAppVersionTemplate	Grants permission to describe application version template	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDraftAppVersionResourcesImportStatus	Grants permission to describe draft application version resources import status	Read	application*		
DescribeMetricsExport	Grants permission to describe metrics export	Read			
DescribeResiliencyPolicy	Grants permission to describe resiliency policy	Read	resiliency-policy*		
DescribeResourceGroupingRecommendationTask	Grants permission to describe the latest status of the grouping recommendation process	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportResourcesToDraftAppVersion	Grants permission to import resources to draft application version	Write	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources
ListAlarmRecommendations	Grants permission to list alarm recommendation	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAppAssessmentComplianceDrifts	Grants permission to list compliance drifts that were detected while running an assessment	List	application*		
ListAppAssessmentResourceDrifts	Grants permission to list resource drifts that were detected while running an assessment	List	application*		
ListAppAssessments	Grants permission to list application assessment	List			
ListAppComponentCompliances	Grants permission to list app component compliances	List	application*		
ListAppComponentRecommendations	Grants permission to list app component recommendations	List	application*		
ListAppInputSources	Grants permission to list application input sources	List	application*		
ListAppVersionAppComponents	Grants permission to list application version app components	List	application*		
ListAppVersionResourceMappings	Grants permission to application version resource mappings	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAppVersionResources	Grants permission to list application resources	List	application*		
ListAppVersions	Grants permission to list application version	List	application*		
ListApps	Grants permission to list applications	List			
ListMetrics	Grants permission to list metrics	List			
ListRecommendationTemplates	Grants permission to list recommendation templates	List	application*		
ListResiliencyPolicies	Grants permission to list resiliency policies	List			
ListResourceGroupingRecommendations	Grants permission to list resource grouping recommendations	List	application*		
ListSopRecommendations	Grants permission to list SOP recommendations	List	application*		
ListSuggestedResiliencyPolicies	Grants permission to list suggested resiliency policies	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a resource	Read			
ListTestRecommendations	Grants permission to list test recommendations	List	application*		
ListUnsupportedAppVersionResources	Grants permission to list unsupported application version resources	List	application*		
PublishAppVersion	Grants permission to publish application version	Write	application*		
PutDraftAppVersionTemplate	Grants permission to put draft application version template	Write	application*		
RejectResourceGroupingRecommendations	Grants permission to reject resource grouping recommendations	Write	application*		
RemoveDraftAppVersionResourceMappings	Grants permission to remove draft application version mappings	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResolveAppVersionResources	Grants permission to resolve application version resources	Write	application*		cloudformation:DescribeStacks cloudformation:ListStackResources resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartAppAssessment	Grants permission to create application assessment	Write	application*		cloudformation:DescribeStacks cloudformation:ListStackResources cloudwatch:DescribeAlarms cloudwatch:GetMetricData cloudwatch:GetMetricStatistics cloudwatch:PutMetricData ec2:DescribeRegions fis:GetExperimentTemplate

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					fis:ListExperimentTemplates fis:ListExperiments resource-groups:GetGroup resource-groups:ListGroupResources servicecatalog:GetApplication servicecatalog:ListAssociatedResources ssm:GetParametersByPath

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
StartMetricsExport	Grants permission to start the metrics export	Write			
StartResourceGroupingRecommendationTask	Grants permission to start the grouping recommendation generation process	Write	application*		
TagResource	Grants permission to assign a resource tag	Tagging	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	app-assessment		
			application		
			recommendation-template		
			resiliency-policy		
				aws:TagKeys	
UpdateApp	Grants permission to update application	Write	application*		iam:PassRole
UpdateAppVersion	Grants permission to update application version	Write	application*		
UpdateAppVersionAppComponent	Grants permission to update application app component	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAppVersionResource	Grants permission to update application resource	Write	application*		
UpdateResiliencyPolicy	Grants permission to update resiliency policy	Write	resiliency-policy*		

Resource types defined by AWS Resilience 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
resiliency-policy	`arn:${Partition}:resiliencehub:${Region}:${Account}:resiliency-policy/${ResiliencyPolicyId}`	aws:ResourceTag/${TagKey}
application	`arn:${Partition}:resiliencehub:${Region}:${Account}:app/${AppId}`	aws:ResourceTag/${TagKey}
app-assessment	`arn:${Partition}:resiliencehub:${Region}:${Account}:app-assessment/${AppAssessmentId}`	aws:ResourceTag/${TagKey}
recommendation-template	`arn:${Partition}:resiliencehub:${Region}:${Account}:recommendation-template/${RecommendationTemplateId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Resilience Hub

AWS Resilience Hub defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) (service prefix: `ram`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Resource Access Manager (RAM)

- Resource types defined by AWS Resource Access Manager (RAM)
- Condition keys for AWS Resource Access Manager (RAM)

Actions defined by AWS Resource Access Manager (RAM)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptResourceShareInvitation	Grants permission to accept the specified resource share invitation	Write	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
AssociateResourceShare	Grants permission to associate resource(s) and/or principal(s) to a resource share	Write	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn ram:RetainSharingOnAccountLeaveOrganization	
AssociateResourceSharePermission	Grants permission to associate a Permission with a Resource Share	Write	customer-managed-permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			permission*		
			resource-share*		
CreatePermission	Grants permission to create a Permission that can be associated to a Resource Share	Write		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	Grants permission to create a new version of a Permission that can be associated to a Resource Share	Write	customer-managed-permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:PermissionArn ram:PermissionResourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResourceShare	Grants permission to create a resource share with provided resource(s) and/or principal(s)	Write		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals ram:RetainSharingOnAccountL	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eaveOrganization	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourceShare	Grants permission to delete resource share	Write	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RetainSharingOnAccountLeaveOrganization	
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 ram:RetainSharingOnAccountL	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eaveOrganization	
DisassociateResourceSharePermission	Grants permission to disassociate a Permission from a Resource Share	Write	customer-managed-permission*		
			permission*		
			resource-share*		
EnableSharingWithAwsOrganization	Grants permission to access customer's organization and create a SLR in the customer's account	Permissions management			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	Grants permission to get the contents of an AWS RAM permission	Read	customer-managed-permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			permission*		
				ram:PermissionArn	
GetResourcePolicies	Grants permission to get the policies for the specified resources that you own and have shared	Read			
GetResourceShareAssociations	Grants permission to get a set of resource share associations from a provided list or with a specified status of the specified type	Read			
GetResourceShareInvitations	Grants permission to get resource share invitations by the specified invitation arn or those for the resource share	Read			
GetResourceShares	Grants permission to get a set of resource shares from a provided list or with a specified status	Read		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPendingInvitationResources	Grants permission to list the resources in a resource share that is shared with you but that the invitation is still pending for	Read	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	Grants permission to list information about the permission and any associations	List	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	Grants permission to list the versions of an AWS RAM permission	List			
ListPermissions	Grants permission to list the AWS RAM permissions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrincipals	Grants permission to list the principals that you have shared resources with or that have shared resources with you	List			
ListReplacePermissionAssociationsWork	Grants permission to retrieve the status of the asynchronous permission replacement	List			
ListResourceSharePermissions	Grants permission to list the Permissions associated with a Resource Share	List	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RetainSharingOnAccountLeaveOrganization	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceTypes	Grants permission to list the shareable resource types supported by AWS RAM	List			
ListResources	Grants permission to list the resources that you added to resource shares or the resources that are shared with you	List			
ListSourceAssociations	Grants permission to list source associations for resource shares	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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectResourceShareInvitation	Grants permission to reject the specified resource share invitation	Write	resource-share-invitation*		
				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 ram:RetainSharingOnAccountLeaveOrganization	

Resource types defined by AWS Resource Access Manager (RAM)

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
resource-share	`arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}`	aws:ResourceTag/${TagKey} ram:AllowsExternalPrincipals ram:ResourceShareName
resource-share-invitation	`arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}`	ram:ShareOwnerAccountId
permission	`arn:${Partition}:ram::${Account}:permission/${ResourcePath}`	ram:PermissionArn ram:PermissionResourceType
customer-managed-permission	`arn:${Partition}:ram:${Region}:${Account}:permission/${ResourcePath}`	aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType

Condition keys for AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request when creating or tagging a resource share. If users don't pass these specific tags, or if they don't specify tags at all, the request fails	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed when creating or tagging a resource share	ArrayOfString
ram:AllowsExternalPrincipals	Filters access by resource shares that allow or deny sharing with external principals. For example, specify true if the action can only be performed on resource shares that allow sharing with external principals. External principals are AWS accounts that are outside of its AWS organization	Bool
ram:PermissionArn	Filters access by the specified Permission ARN	ARN
ram:PermissionResourceType	Filters access by permissions of specified resource type	String
ram:Principal	Filters access by format of the specified principal	String

Condition keys	Description	Type
ram:RequestedAllowsExternalPrincipals	Filters access by the specified value for 'allowExternalPrincipals'. External principals are AWS accounts that are outside of its AWS Organization	Bool
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:RetainSharingOnAccountLeaveOrganization	Filters access by RetainSharingOnAccountLeaveOrganization value within ResourceShareConfiguration that is set on resource share	Bool
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 AWS Resource Explorer

AWS Resource Explorer (service prefix: `resource-explorer-2`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Resource Explorer

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDefaultView	Grants permission to set the specified view as the default for this AWS Region in this AWS account	Write			
BatchGetView	Grants permission to retrieve details about views that you specify by a list of ARNs	Read			resource-explorer-2:GetView
CreateIndex	Grants permission to turn on Resource Explorer in the AWS Region in which you called	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	this operation by creating an index			aws:TagKeys	
CreateManagedView [permission only]	Grants permission to create managed view	Write			
CreateResourceExplorerSetup	Grants permission to create resource explorer setup	Write			
CreateStreamingAccessForService [permission only]	Grants permission to create resource explorer streaming access	Write			
CreateView	Grants permission to create a view that users can query	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIndex	Grants permission to turn off Resource Explorer in the specified AWS Region by deleting the index	Write	index*		
DeleteResourceExplorerSetup	Grants permission to delete resource explorer setup	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy [permission only]	Grants permission to delete the specified view's resource policy	Permissions management	view*		
DeleteStreamingAccessForService [permission only]	Grants permission to delete resource explorer streaming access	Write			
DeleteView	Grants permission to delete a view	Write	view*		
DisassociateDefaultView	Grants permission to remove the default view for the AWS Region in which you call this operation	Write			
GetAccountLevelServiceConfiguration	Grants permission to Resource Explorer to access account level data within your AWS Organization	Read			
GetDefaultView	Grants permission to retrieve the Amazon resource name (ARN) of the view that is the default for the AWS Region in which you call this operation	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIndex	Grants permission to retrieve information about the index in the AWS Region in which you call this operation	Read			
GetManagedView	Grants permission to get managed view	Read	managed-view*		
GetResourceExplorerSetup	Grants permission to get resource explorer setup	Read			
GetResourcePolicy [permission only]	Grants permission to retrieve information about the specified view's resource policy	Read	view*		
GetServiceIndex	Grants permission to get service index	Read			
GetServiceView	Grants permission to get service view	Read			
GetView	Grants permission to retrieve information about the specified view	Read	view*		
ListIndexes	Grants permission to list the indexes in all AWS Regions	List			
ListIndexesForMembers	Grants permission to list the organization member account's indexes in all AWS Regions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListManagedViews	Grants permission to list managed views	List			
ListServiceIndexes	Grants permission to list service indexes in all AWS Regions	List			
ListServiceViews	Grants permission to list service views in all AWS Regions	List			
ListStreamingAccessForServices	Grants permission to list streaming access for services	List			
ListSupportedResourceTypes	Grants permission to retrieve a list of all resource types currently supported by Resource Explorer	List			
ListTagsForResource	Grants permission to list the tags that are attached to the specified resource	Read	index view		
ListViews	Grants permission to list the Amazon resource names (ARNs) of all of the views available in the AWS Region in which you call this operation	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy [permission only]	Grants permission to update the specified view's resource policy	Permissions management	view*		
Search	Grants permission to search for resources and display details about all resources that match the specified criteria	Read	view*		
				resource-explorer-2:Operation	
TagResource	Grants permission to add one or more tag key and value pairs to the specified resource	Tagging	index		
			view		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tag key and value pairs from the specified resource	Tagging	index		
			view		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIndexType	Grants permission to change the type of the index from LOCAL to AGGREGATOR or back	Write	index*		
UpdateView	Grants permission to modify some of the details of a view	Write	view*		

Resource types defined by AWS Resource Explorer

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
view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${ViewUuid}`	aws:ResourceTag/${TagKey}
index	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${IndexUuid}`	aws:ResourceTag/${TagKey}
managed-view	`arn:${Partition}:resource-explorer-2:${Region}:${Account}:managed-view/${ManagedViewName}/${ManagedViewUuid}`	

Condition keys for AWS Resource Explorer

AWS Resource Explorer defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag keys that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag keyss attached to the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
resource-explorer-2:Operation	Filters access by the actual operation that is being invoked, available values: Search, ListResources	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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReportCreation	Grants permission to describe the status of the StartReportCreation operation	Read			
GetComplianceSummary	Grants permission to retrieve a summary of how many resources are noncompliant with their effective tag policies	Read			
GetResources	Grants permission to return tagged or previously tagged resources in the specified AWS Region for the calling account	Read			
GetTagKeys	Grants permission to returns tag keys currently in use in the specified AWS Region for the calling account	Read			
GetTagValues	Grants permission to return tag values for the specified	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	key that are used in the specified AWS Region for the calling account				
ListRequiredTags	Grants permission to list required tags for supported resource types in the calling account	List			
StartReportCreation	Grants permission to start generating a report listing all tagged resources in accounts across your organization, and whether each resource is compliant with the effective tag policy	Write			
TagResources	Grants permission to apply one or more tags to the specified resources	Tagging			
UntagResources	Grants permission to remove the specified tags from the specified resources	Tagging			

Resource types defined by Amazon Resource Group Tagging API

Amazon Resource Group Tagging API does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Resource Group Tagging API, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Resource Group Tagging API

Resource Group Tagging has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Resource Groups

AWS Resource Groups (service prefix: `resource-groups`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Resource Groups
- Resource types defined by AWS Resource Groups
- Condition keys for AWS Resource Groups

Actions defined by AWS Resource Groups

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Resource [permission only]	Grants permission to associate a resource to an Application	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTagSyncTask	Grants permission to cancel a tag-sync task for an application group	Write	group*		resource-groups:DeleteGroup
CreateGroup	Grants permission to create a resource group with a specified name, description, and resource query	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	Grants permission to delete a specified resource group	Write	group*		tag:GetResources
DeleteGroupPolicy [permission only]	Grants permission to delete a resource-based policy for the specified group	Write	group*		
DisassociateResource [permission only]	Grants permission to disassociate a resource from an Application	Write	group*		
GetAccountSettings	Grants permission to get the current status of optional features in Resource Groups	Read			
GetGroup	Grants permission to get information of a specified resource group	Read	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupConfiguration	Grants permission to get the service configuration associated with the specified resource group	Read	group*		
GetGroupPolicy [permission only]	Grants permission to get a resource-based policy for the specified group	Read	group*		
GetGroupQuery	Grants permission to get the query associated with a specified resource group	Read	group*		
GetTagSyncTask	Grants permission to get information of a specified tag-sync task	Read	group*		
GetTags	Grants permission to get the tags associated with a specified resource group	Read	group*		
GroupResources	Grants permission to add the specified resources to the specified group	Write	group*		resource-groups:Tag tag:TagResources

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGroupResources	Grants permission to list the resources that are members of a specified resource group	List	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	Grants permission to list grouping statuses for a specified application group	List	group*		
ListGroups	Grants permission to list all resource groups in your account	List			
ListResourceTypes [permission only]	Grants permission to list supported resource types	List			
ListTagSyncTasks	Grants permission to list all tag-sync tasks in your account	List	group*		
PutGroupConfiguration	Grants permission to put the service configuration associated with the specified resource group	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutGroupPolicy [permission only]	Grants permission to add a resource-based policy for the specified group	Write	group*		
SearchResources	Grants permission to search for AWS resources matching the given query	List			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
StartTagSyncTask	Grants permission to create a tag-sync task for an application group	Write	group*		iam:PassRole resource-groups:CreateGroup
Tag	Grants permission to tag a specified resource group	Tagging	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UngroupResources	Grants permission to remove the specified resources from the specified group	Write	group*		resource-groups:Untag tag:UntagResources
Untag	Grants permission to remove tags associated with a specified resource group	Tagging	group*		
				aws:TagKeys	
UpdateAccountSettings	Grants permission to update optional features in Resource Groups	Write			
UpdateGroup	Grants permission to update a specified resource group	Write	group*		
UpdateGroupQuery	Grants permission to update the query associated with a specified resource group	Write	group*		cloudformation:DescribeStacks

Resource types defined by AWS Resource Groups

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
group	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}	aws:ResourceTag/${TagKey}
tagSyncTask	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}/tag-sync-task/${TaskId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Resource Groups

AWS Resource Groups defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon RHEL Knowledgebase Portal

Amazon RHEL Knowledgebase Portal (service prefix: rhelkb) 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 RHEL Knowledgebase 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRhelURL	Grants permission to access the Red Hat Knowledgebase portal	Read			

Resource types defined by Amazon RHEL Knowledgebase Portal

Amazon RHEL Knowledgebase Portal does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon RHEL Knowledgebase Portal, specify `"Resource": "*"` in your policy.

Condition keys for Amazon RHEL Knowledgebase Portal

RHEL KB has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS RoboMaker

AWS RoboMaker (service prefix: `robomaker`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS RoboMaker
- Resource types defined by AWS RoboMaker
- Condition keys for AWS RoboMaker

Actions defined by AWS RoboMaker

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteWorlds	Delete one or more worlds in a batch operation	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDescribeSimulationJob	Describe multiple simulation jobs	Read			
CancelDeploymentJob	Cancel a deployment job	Write	deploymentJob*		
CancelSimulationJob	Cancel a simulation job	Write	simulationJob*		
CancelSimulationJobBatch	Cancel a simulation job batch	Write	simulationJobBatch*		
CancelWorldExportJob	Cancel a world export job	Write	worldExportJob*		
CancelWorldGenerationJob	Cancel a world generation job	Write	worldGenerationJob*		
CreateDeploymentJob	Create a deployment job	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFleet	Create a deployment fleet that represents a logical group of robots running the same robot application	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobot	Create a robot that can be registered to a fleet	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateRobotApplication	Create a robot application	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateRobotApplicationVersion	Create a snapshot of a robot application	Write	robotApplication*		s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSimulationApplication	Create a simulation application	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreateSimulationApplicationVersion	Create a snapshot of a simulation application	Write	simulationApplication*		s3:GetObject
CreateSimulationJob	Create a simulation job	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole
CreateWorldExportJob	Create a world export job	Write	world*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldGenerationJob	Create a world generation job	Write	worldTemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWorldTemplate	Create a world template	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteFleet	Delete a deployment fleet	Write	deploymentFleet*		
DeleteRobot	Delete a robot	Write	robot*		
DeleteRobotApplication	Delete a robot application	Write	robotApplication*		
DeleteSimulationApplication	Delete a simulation application	Write	simulationApplication*		
DeleteWorldTemplate	Delete a world template	Write	worldTemplate*		
DeregisterRobot	Deregister a robot from a fleet	Write	deploymentFleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			robot*		
DescribeDeploymentJob	Describe a deployment job	Read	deploymentJob*		
DescribeFleet	Describe a deployment fleet	Read	deploymentFleet*		
DescribeRobot	Describe a robot	Read	robot*		
DescribeRobotApplication	Describe a robot application	Read	robotApplication*		
DescribeSimulationApplication	Describe a simulation application	Read	simulationApplication*		
DescribeSimulationJob	Describe a simulation job	Read	simulationJob*		
DescribeSimulationJobBatch	Describe a simulation job batch	Read	simulationJobBatch*		
DescribeWorld	Describe a world	Read	world*		
DescribeWorldExportJob	Describe a world export job	Read	worldExportJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWorldGenerationJob	Describe a world generation job	Read	worldGenerationJob*		
DescribeWorldTemplate	Describe a world template	Read	worldTemplate*		
GetWorldTemplateBody	Get the body of a world template	Read	worldTemplate*		
ListDeploymentJobs	List deployment jobs	List			
ListFleets	List fleets	List			
ListRobotApplications	List robot applications	List			
ListRobots	List robots	List			
ListSimulationApplications	List simulation applications	List			
ListSimulationJobBatches	List simulation job batches	List			
ListSimulationJobs	List simulation jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSupportedAvailabilityZones [permission only]	Lists supported availability zones	List			
ListTagsForResource	List tags for a RoboMaker resource	List	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			worldTemplate		
ListWorldExportJobs	List world export jobs	List			
ListWorldGenerationJobs	List world generation jobs	List			
ListWorldTemplates	List world templates	List			
ListWorlds	List worlds	List			
RegisterRobot	Register a robot to a fleet	Write	deploymentFleet*		
			robot*		
RestartSimulationJob	Restart a running simulation job	Write	simulationJob*		
StartSimulationJobBatch	Create a simulation job batch	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SyncDeploymentJob	Ensures the most recently deployed robot application is deployed to all robots in the fleet	Write	deploymentFleet*		iam:CreateServiceLinkedRole
TagResource	Add tags to a RoboMaker resource	Tagging	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		
			worldExportJob		
			worldGenerationJob		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			worldTemplate		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Remove tags from a RoboMaker resource	Tagging	deploymentFleet		
			deploymentJob		
			robot		
			robotApplication		
			simulationApplication		
			simulationJob		
			simulationJobBatch		
			world		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			worldExportJob		
			worldGenerationJob		
			worldTemplate		
				aws:TagKeys	
UpdateRobotApplication	Update a robot application	Write	robotApplication*		
UpdateRobotDeployment [permission only]	Report the deployment status for an individual robot	Write			
UpdateSimulationApplication	Update a simulation application	Write	simulationApplication*		
UpdateWorldTemplate	Update a world template	Write	worldTemplate*		

Resource types defined by AWS RoboMaker

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
robotApplication	arn:${Partition}:robomaker:${Region}:${Account}:robot-application/${ApplicationName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
simulationApplication	arn:${Partition}:robomaker:${Region}:${Account}:simulation-application/${ApplicationName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
simulationJob	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job/${SimulationJobId}	aws:ResourceTag/${TagKey}
simulationJobBatch	arn:${Partition}:robomaker:${Region}:${Account}:simulation-job-batch/${SimulationJobBatchId}	aws:ResourceTag/${TagKey}
deploymentJob	arn:${Partition}:robomaker:${Region}:${Account}:deployment-job/${DeploymentJobId}	aws:ResourceTag/${TagKey}
robot	arn:${Partition}:robomaker:${Region}:${Account}:robot/${RobotName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
deploymentFleet	arn:${Partition}:robomaker:${Region}:${Account}:deployment-fleet/${FleetName}/${CreatedOnEpoch}	aws:ResourceTag/${TagKey}
worldGenerationJob	arn:${Partition}:robomaker:${Region}:${Account}:world-generation-job/${WorldGenerationJobId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
worldExportJob	arn:${Partition}:robomaker:${Region}:${Account}:world-export-job/${WorldExportJobId}	aws:ResourceTag/${TagKey}
worldTemplate	arn:${Partition}:robomaker:${Region}:${Account}:world-template/${WorldTemplateJobId}	aws:ResourceTag/${TagKey}
world	arn:${Partition}:robomaker:${Region}:${Account}:world/${WorldId}	aws:ResourceTag/${TagKey}

Condition keys for AWS RoboMaker

AWS RoboMaker defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateKeySigningKey	Grants permission to activate a key-signing key so that it can be used for signing by DNSSEC	Write	hostedzone*		
AssociateVPCWithHostedZone	Grants permission to associate an additional Amazon VPC with a private hosted zone	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:ChangeResourceRecordSetsActions	
ChangeTagsForResource	Grants permission to add, edit, or delete tags for a health check or a hosted zone	Tagging	healthcheck*		
			hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
CreateQueryLoggingConfig	Grants permission to create a configuration for DNS query logging	Write	hostedzone*		
CreateReusableDelegationSet	Grants permission to create a delegation set (a group of four name servers) that can be reused by multiple hosted zones	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficPolicy	Grants permission to create a traffic policy, which you use to create multiple DNS records for one domain name (such as example.com) or one subdomain name (such as www.example.com)	Write			
CreateTrafficPolicyInstance	Grants permission to create records in a specified hosted zone based on the settings in a specified traffic policy version	Write	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	Grants permission to create a new version of an existing traffic policy	Write	trafficpolicy*		
CreateVPCAssociationAuthorization	Grants permission to authorize the AWS account that created a specified VPC to submit an Associate VPCWithHostedZone request, which associates the VPC with a specified hosted zone that was created by a different account	Write	hostedzone* 	 route53:VPCs	
DeactivateKeySigningKey	Grants permission to deactivate a key-signing key so that it will not be used for signing by DNSSEC	Write	hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCidrCollection	Grants permission to delete a CIDR collection	Write	cidrcollection*		
DeleteHealthCheck	Grants permission to delete a health check	Write	healthcheck*		
DeleteHostedZone	Grants permission to delete a hosted zone	Write	hostedzone*		
DeleteKeySigningKey	Grants permission to delete a key-signing key	Write	hostedzone*		
DeleteQueryLoggingConfig	Grants permission to delete a configuration for DNS query logging	Write	queryloggingconfig*		
DeleteReusableDelegationSet	Grants permission to delete a reusable delegation set	Write	delegationset*		
DeleteTrafficPolicy	Grants permission to delete a traffic policy	Write	trafficpolicy*		
DeleteTrafficPolicyInstance	Grants permission to delete a traffic policy instance and all the records that Route 53 created when you created the instance	Write	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Grants permission to remove authorization for associating an Amazon Virtual Private Cloud with a Route 53 private hosted zone	Write	hostedzone*		
				route53:VPCs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableHostedZoneDNSSEC	Grants permission to disable DNSSEC signing in a specific hosted zone	Write	hostedzone*		
DisassociateVPCFromHostedZone	Grants permission to disassociate an Amazon Virtual Private Cloud from a Route 53 private hosted zone	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
EnableHostedZoneDNSSEC	Grants permission to enable DNSSEC signing in a specific hosted zone	Write	hostedzone*		
GetAccountLimit	Grants permission to get the specified limit for the current account, for example, the maximum number of health checks that you can create using the account	Read			
GetChange	Grants permission to get the current status of a request to create, update, or delete one or more records	List	change*		
GetCheckerIpRanges	Grants permission to get a list of the IP ranges that are used by Route 53 health checkers to check the health of your resources	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDNSSEC	Grants permission to get information about DNSSEC for a specific hosted zone, including the key-signing keys in the hosted zone	Read	hostedzone*		
GetGeoLocation	Grants permission to get information about whether a specified geographic location is supported for Route 53 geolocation records	List			
GetHealthCheck	Grants permission to get information about a specified health check	Read	healthcheck*		
GetHealthCheckCount	Grants permission to get the number of health checks that are associated with the current AWS account	List			
GetHealthCheckLastFailureReason	Grants permission to get the reason that a specified health check failed most recently	List	healthcheck*		
GetHealthCheckStatus	Grants permission to get the status of a specified health check	List	healthcheck*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHostedZone	Grants permission to get information about a specified hosted zone including the four name servers that Route 53 assigned to the hosted zone	List	hostedzone*		
GetHostedZoneCount	Grants permission to get the number of hosted zones that are associated with the current AWS account	List			
GetHostedZoneLimit	Grants permission to get the specified limit for a specified hosted zone	Read	hostedzone*		
GetQueryLoggingConfig	Grants permission to get information about a specified configuration for DNS query logging	Read	queryloggingconfig*		
GetReusableDelegationSet	Grants permission to get information about a specified reusable delegation set, including the four name servers that are assigned to the delegation set	List	delegationset*		
GetReusableDelegationSetLimit	Grants permission to get the maximum number of hosted zones that you can associate with the specified reusable delegation set	Read	delegationset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrafficPolicy	Grants permission to get information about a specified traffic policy version	Read	trafficpolicy*		
GetTrafficPolicyInstance	Grants permission to get information about a specified traffic policy instance	Read	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	Grants permission to get the number of traffic policy instances that are associated with the current AWS account	Read			
ListCidrBlocks	Grants permission to get a list of the CIDR blocks within a specified CIDR collection	List	cidrcollection*		
ListCidrCollections	Grants permission to get a list of the CIDR collections that are associated with the current AWS account	List			
ListCidrLocations	Grants permission to get a list of the CIDR locations that belong to a specified CIDR collection	List	cidrcollection*		
ListGeoLocations	Grants permission to get a list of geographic locations that Route 53 supports for geolocation	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHealthChecks	Grants permission to get a list of the health checks that are associated with the current AWS account	Read			
ListHostedZones	Grants permission to get a list of the public and private hosted zones that are associated with the current AWS account	List			
ListHostedZonesByName	Grants permission to get a list of your hosted zones in lexicographic order. Hosted zones are sorted by name with the labels reversed, for example, com.example.www	List			
ListHostedZonesByVPC	Grants permission to get a list of all the private hosted zones that a specified VPC is associated with	List		route53:VPCs	ec2:DescribeVpcs
ListQueryLoggingConfigs	Grants permission to list the configurations for DNS query logging that are associated with the current AWS account or the configuration that is associated with a specified hosted zone	List	hostedzone		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceRecordSets	Grants permission to list the records in a specified hosted zone	List	hostedzone*		
ListReusableDelegationSets	Grants permission to list the reusable delegation sets that are associated with the current AWS account.	Read			
ListTagsForResource	Grants permission to list tags for one health check or hosted zone	Read	healthcheck		
			hostedzone		
ListTagsForResources	Grants permission to list tags for up to 10 health checks or hosted zones	Read	healthcheck		
			hostedzone		
ListTrafficPolicies	Grants permission to get information about the latest version for every traffic policy that is associated with the current AWS account. Policies are listed in the order in which they were created	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrafficPolicyInstances	Grants permission to get information about the traffic policy instances that you created by using the current AWS account	Read			
ListTrafficPolicyInstancesByHostedZone	Grants permission to get information about the traffic policy instances that you created in a specified hosted zone	List	hostedzone*		
ListTrafficPolicyInstancesByPolicy	Grants permission to get information about the traffic policy instances that you created using a specified traffic policy version	List	trafficpolicy*		
ListTrafficPolicyVersions	Grants permission to get information about all the versions for a specified traffic policy	List	trafficpolicy*		
ListVPCAssociationAuthorizations	Grants permission to get a list of the VPCs that were created by other accounts and that can be associated with a specified hosted zone	List	hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestDNSAnswer	Grants permission to get the value that Route 53 returns in response to a DNS query for a specified record name and type	Read			
UpdateHealthCheck	Grants permission to update an existing health check	Write	healthcheck*		
UpdateHostedZoneComment	Grants permission to update the comment for a specified hosted zone	Write	hostedzone*		
UpdateHostedZoneFeatures	Grants permission to update features for a specified hosted zone	Write	hostedzone*		
UpdateTrafficPolicyComment	Grants permission to update the comment for a specified traffic policy version	Write	trafficpolicy*		
UpdateTrafficPolicyInstance	Grants permission to update the records in a specified hosted zone that were created based on the settings in a specified traffic policy version	Write	trafficpolicyinstance*		

Resource types defined by Amazon Route 53

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cidrcollection	arn:${Partition}:route53:::cidrcollection/${Id}	
change	arn:${Partition}:route53:::change/${Id}	
delegationset	arn:${Partition}:route53:::delegationset/${Id}	
healthcheck	arn:${Partition}:route53:::healthcheck/${Id}	
hostedzone	arn:${Partition}:route53:::hostedzone/${Id}	
trafficpolicy	arn:${Partition}:route53:::trafficpolicy/${Id}	
trafficpolicyinstance	arn:${Partition}:route53:::trafficpolicyinstance/${Id}	
queryloggingconfig	arn:${Partition}:route53:::queryloggingconfig/${Id}	
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	

Condition keys for Amazon Route 53

Amazon Route 53 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
route53:ChangeResourceRecordSetsActions	Filters access by the change actions, CREATE, UPSERT, or DELETE, in a ChangeResourceRecordSets request	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	Filters access by the normalized DNS record names in a ChangeResourceRecordSets request	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	Filters access by the DNS record types in a ChangeResourceRecordSets request	ArrayOfString
route53:VPCs	Filters access by VPCs in request	String

Actions, resources, and condition keys for Amazon Route 53 Domains

Amazon Route 53 Domains (service prefix: `route53domains`) 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 Domains

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDomainTransferFromAnotherAwsAccount	Grants permission to accept the transfer of a domain from another AWS account to the current AWS account	Write			
AssociateDelegationSignerToDomain	Grants permission to associate a new delegation signer to a domain	Write			
CancelDomainTransferToAnotherAwsAccount	Grants permission to cancel the transfer of a domain from the current AWS account to another AWS account	Write			
CheckDomainAvailability	Grants permission to check the availability of one domain name	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckDomainTransferability	Grants permission to check whether a domain name can be transferred to Amazon Route 53	Read			
DeleteDomain	Grants permission to delete domains	Write			
DeleteTagsForDomain	Grants permission to delete the specified tags for a domain	Tagging			
DisableDomainAutoRenew	Grants permission to configure Amazon Route 53 to automatically renew the specified domain before the domain registration expires	Write			
DisableDomainTransferLock	Grants permission to remove the transfer lock on the domain (specifically the clientTransferProhibited status) to allow domain transfers	Write			
DisassociateDelegationSignerFromDomain	Grants permission to disassociate an existing delegation signer from a domain	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableDomainAutoRenew	Grants permission to configure Amazon Route 53 to automatically renew the specified domain before the domain registration expires	Write			
EnableDomainTransferLock	Grants permission to set the transfer lock on the domain (specifically the clientTransferProhibited status) to prevent domain transfers	Write			
GetContactReachabilityStatus	Grants permission to get information about whether the registrant contact has responded for operations that require confirmation that the email address for the registrant contact is valid, such as registering a new domain	Read			
GetDomainDetail	Grants permission to get detailed information about a domain	Read			
GetDomainSuggestions	Grants permission to get a list of suggested domain names given a string, which can either be a domain name or simply a word or phrase (without spaces)	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOperationDetail	Grants permission to get the current status of an operation that is not completed	Read			
ListDomains	Grants permission to list all the domain names registered with Amazon Route 53 for the current AWS account	List			
ListOperations	Grants permission to list the operation IDs of operations that are not yet complete	List			
ListPrices	Grants permission to list the prices of operations for TLDs	List			
ListTagsForDomain	Grants permission to list all the tags that are associated with the specified domain	Read			
PushDomain	Grants permission to change the IPS tag of .uk domain to initiate a transfer process from Route 53 to another registrar	Write			
RegisterDomain	Grants permission to register domains	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectDomainTransferFromAnotherAwsAccount	Grants permission to reject the transfer of a domain from another AWS account to the current AWS account	Write			
RenewDomain	Grants permission to renew domains for the specified number of years	Write			
ResendContactReachabilityEmail	Grants permission to resend the confirmation email to the current email address for the registrant contact for operations that require confirmation that the email address for the registrant contact is valid, such as registering a new domain	Write			
ResendOperationAuthorization	Grants permission to resend the operation authorization	Write			
RetrieveDomainAuthCode	Grants permission to get the AuthCode for the domain	Write			
TransferDomain	Grants permission to transfer a domain from another registrar to Amazon Route 53	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TransferDomainToAnotherAwsAccount	Grants permission to transfer a domain from the current AWS account to another AWS account	Write			
UpdateDomainContact	Grants permission to update the contact information for domain	Write			
UpdateDomainContactPrivacy	Grants permission to update the domain contact privacy setting	Write			
UpdateDomainNameservers	Grants permission to replace the current set of name servers for a domain with the specified set of name servers	Write			
UpdateTagsForDomain	Grants permission to add or update tags for a specified domain	Tagging			
ViewBilling	Grants permission to get all the domain-related billing records for the current AWS account for a specified period	Read			

Resource types defined by Amazon Route 53 Domains

Amazon Route 53 Domains does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Route 53 Domains, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Route 53 Domains

Route 53 Domains has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate 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 route53profiles:ResourceIds	
AssociateResourceToProfile	Grants permission to associates a resource, such as DNS Firewall rule group, private hosted zone, resolver rule, etc. to a specified Profile	Write		route53profiles:ResourceTypes route53profiles:HostedZoneDomains route53profiles:ResolverRuleDomains route53profiles:FirewallRuleGroupPriority route53profiles:ResourceArns	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		route53profiles:ResourceIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		route53profiles:ResourceTypes route53profiles:HostedZoneDomains route53profiles:ResolverRuleDomains route53profiles:FirewallRuleGroupPriority route53profiles:ResourceArns	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		route53profiles:ResourceTypes route53profiles:HostedZoneDomains route53profiles:ResolverRuleDomains route53profiles:FirewallRuleGroupPriority	

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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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
route53profiles:FirewallRuleGroupPriority	Filters access by priority range of a Firewall Rule Group	Numeric
route53profiles:Ho	Filters access by Hosted Zone domains	String

Condition keys	Description	Type
stedZoneDomains		
route53profiles:ResolverRuleDomains	Filters access by Resolver Rule domains	String
route53profiles:ResourceArns	Filters access by specific resource ARNs	ARN
route53profiles:ResourceIds	Filters access by given VPCs	String
route53profiles:ResourceTypes	Filters access by specific resource type. Possible options include 'HostedZone', 'FirewallRuleGroup', 'Resolver QueryLoggingConfig', 'ResolverRule', and 'VpcEndpoint'	String

Actions, resources, and condition keys for Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster (service prefix: `route53-recovery-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 Amazon Route 53 Recovery Cluster

- Resource types defined by Amazon Route 53 Recovery Cluster
- Condition keys for Amazon Route 53 Recovery Cluster

Actions defined by Amazon Route 53 Recovery Cluster

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRoutingControlState	Grants permission to get a routing control state	Read	routingcontrol*		
ListRoutingControls	Grants permission to list routing controls	Read			
UpdateRoutingControlState	Grants permission to update a routing control state	Write	routingcontrol*		
				route53-recovery-cluster:AllowSafetyRulesOverrides	
UpdateRoutingControlStates	Grants permission to update a batch of routing control states	Write	routingcontrol*		
				route53-recovery-cluster:Al	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lowSafetyRulesOverrides	

Resource types defined by Amazon Route 53 Recovery Cluster

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
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	

Condition keys for Amazon Route 53 Recovery Cluster

Amazon Route 53 Recovery Cluster defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
route53-recovery-cluster:AllowSafetyRulesOverrides	Override safety rules to allow routing control state updates	Bool

Actions, resources, and condition keys for Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls (service prefix: `route53-recovery-control-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 Route 53 Recovery Controls

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateControlPanel	Grants permission to create a control panel	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRoutingControl	Grants permission to create a routing control	Write	cluster*		
CreateSafetyRule	Grants permission to create a safety rule	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Grants permission to delete a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteControlPanel	Grants permission to delete a control panel	Write	controlpanel*		
DeleteResourcePolicy [permission only]	Grants permission to delete the RAM access control policy for a cluster	Permissions management	cluster*		
DeleteRoutingControl	Grants permission to delete a routing control	Write	routingcontrol*		
DeleteSafetyRule	Grants permission to delete a safety rule	Write	safetyrule*		
DescribeCluster	Grants permission to describe a cluster	Read	cluster*		
DescribeControlPanel	Grants permission to describe a control panel	Read	controlpanel*		
DescribeRoutingControl	Grants permission to describe a routing control	Read	routingcontrol*		
DescribeSafetyRule	Grants permission to describe a safety rule	Read	safetyrule*		
GetResourcePolicy	Grants permission to get the resource policy of a cluster	Read	cluster*		
ListAssociatedRoute53HealthChecks	Grants permission to list associated Route 53 health checks	List	routingcontrol*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClusters	Grants permission to list clusters	Read			
ListControlPanels	Grants permission to list control panels	Read			
ListRoutingControls	Grants permission to list routing controls	Read	controlpanel*		
ListSafetyRules	Grants permission to list safety rules	Read	controlpanel*		
ListTagsForResource	Grants permission to list tags for a resource	Read	cluster		
			controlpanel		
			safetyrule		
PutResourcePolicy [permission only]	Grants permission to define the RAM access control policy for a cluster	Permissions management	cluster*		
TagResource	Grants permission to tag a resource	Tagging	cluster		
			controlpanel		
			safetyrule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	cluster		
			controlpanel		
			safetyrule		
				aws:TagKeys	
UpdateCluster	Grants permission to update a cluster	Write	cluster*		
UpdateControlPanel	Grants permission to update a cluster	Write	controlpanel*		
UpdateRoutingControl	Grants permission to update a routing control	Write	routingcontrol*		
UpdateSafetyRule	Grants permission to update a safety rule	Write	safetyrule*		

Resource types defined by Amazon Route 53 Recovery Controls

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:${Partition}:route53-recovery-control::${Account}:cluster/${ResourceId}`	aws:ResourceTag/${TagKey}
controlpanel	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}`	aws:ResourceTag/${TagKey}
routingcontrol	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/routingcontrol/${RoutingControlId}`	
safetyrule	`arn:${Partition}:route53-recovery-control::${Account}:controlpanel/${ControlPanelId}/safetyrule/${SafetyRuleId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Route 53 Recovery Controls

Amazon Route 53 Recovery Controls defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag's key and value in a request	String
aws:ResourceTag/${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 Recovery Readiness

Amazon Route 53 Recovery Readiness (service prefix: `route53-recovery-readiness`) 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 Recovery Readiness
- Resource types defined by Amazon Route 53 Recovery Readiness
- Condition keys for Amazon Route 53 Recovery Readiness

Actions defined by Amazon Route 53 Recovery Readiness

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCell	Grants permission to create a new cell	Write	cell*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrossAccountAuthorization	Grants permission to create a cross account authorization	Write			
CreateReadinessCheck	Grants permission to create a readiness check	Write	readinesscheck*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecoveryGroup	Grants permission to create a recovery group	Write	recoverygroup*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateResourceSet	Grants permission to create a resource set	Write	resourceset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCell	Grants permission to delete a cell	Write	cell*		
DeleteCrossAccountAuthorization	Grants permission to delete a cross account authorization	Write			
DeleteReadinessCheck	Grants permission to delete a readiness check	Write	readinesscheck*		
DeleteRecoveryGroup	Grants permission to delete a recovery group	Write	recoverygroup*		
DeleteResourceSet	Grants permission to delete a resource set	Write	resourceset*		
GetArchitectureRecommendations	Grants permission to get architecture recommendations for a recovery group	Read	recoverygroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCell	Grants permission to get information about a cell	Read	cell*		
GetCellReadinessSummary	Grants permission to get a readiness summary for a cell	Read	cell*		
GetReadinessCheck	Grants permission to get information about a readiness check	Read	readinesscheck*		
GetReadinessCheckResourceStatus	Grants permission to get the readiness status for an individual resource	Read	readinesscheck*		
GetReadinessCheckStatus	Grants permission to get the status of a readiness check (for a resource set)	Read	readinesscheck*		
GetRecoveryGroup	Grants permission to get information about a recovery group	Read	recoverygroup*		
GetRecoveryGroupReadinessSummary	Grants permission to get a readiness summary for a recovery group	Read	recoverygroup*		
GetResourceSet	Grants permission to get information about a resource set	Read	resourceset*		
ListCells	Grants permission to list cells	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCrossAccountAuthorizations	Grants permission to list cross account authorizations	Read			
ListReadinessChecks	Grants permission to list readiness checks	Read			
ListRecoveryGroups	Grants permission to list recovery groups	Read			
ListResourceSets	Grants permission to list resource sets	Read			
ListRules	Grants permission to list readiness rules	Read			
ListTagsForResources	Grants permission to list tags for a resource	Read			
TagResource	Grants permission to add a tag to a resource	Tagging	cell		
			readinesscheck		
			recoverygroup		
			resourceset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag from a resource	Tagging	cell		
			readinesscheck		
			recoverygroup		
			resourceset		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateCell	Grants permission to update a cell	Write	cell*		
				aws:TagKeys	
UpdateReadinessCheck	Grants permission to update a readiness check	Write	readinesscheck*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateRecoveryGroup	Grants permission to update a recovery group	Write	recoverygroup*		
				aws:TagKeys	
UpdateResourceSet	Grants permission to update a resource set	Write	resourceset*		
				aws:TagKeys	

Resource types defined by Amazon Route 53 Recovery Readiness

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
readinesscheck	`arn:${Partition}:route53-recovery-readiness::${Account}:readiness-check/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
resourceset	arn:${Partition}:route53-recovery-readiness::${Account}:resource-set/${ResourceId}	aws:ResourceTag/${TagKey}
cell	arn:${Partition}:route53-recovery-readiness::${Account}:cell/${ResourceId}	aws:ResourceTag/${TagKey}
recoverygroup	arn:${Partition}:route53-recovery-readiness::${Account}:recovery-group/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Route 53 Recovery Readiness

Amazon Route 53 Recovery Readiness defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFirewallRuleGroup	Grants permission to associate an Amazon VPC with a specified firewall rule group	Write	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Grants permission to create a Firewall rule within a Firewall rule group	Write	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	Grants permission to create a Firewall rule group	Write	firewall-rule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutpostResolver	Grants permission to create a Route 53 Resolver on Outposts	Write	outpost-resolver*		outposts:GetOutpost

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverQueryLogConfig	Grants permission to create a Resolver query logging configuration, which defines where you want Resolver to save DNS query logs that originate in your VPCs	Write	resolver-query-log-config*		
				aws:RequestTag/${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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 AWS 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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResolverDnssecConfig	Grants permission to get the DNSSEC validation support status for DNS queries within the specified resource	Read	resolver-dnssec-config*		
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 AWS 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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account to use	Read	resolver-rule*		
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 AWS account is able to check	List			ec2:DescribeVpcs
ListFirewallDomainLists	Grants permission to list all the Firewall domain list that current AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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*		
ListOutpostResolvers	Grants permission to list all instances of Route 53 Resolver on Outposts that were created using the current AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResolverEndpoints	Grants permission to list all the Resolver endpoints that were created using the current AWS account	List			
ListResolverQueryLogConfigAssociations	Grants permission to list information about associations between Amazon VPCs and query logging configurations	List			ec2:DescribeVpcs
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 AWS account	List			ec2:DescribeVpcs
ListResolverRules	Grants permission to list the Resolver rules that were created using the current AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags that you associated with the specified resource	Read	firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFirewallRuleGroupPolicy	Grants permission to specify an AWS 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*		
PutResolverQueryLogConfigPolicy	Grants permission to specify an AWS 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 AWS 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		

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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a specified resource	Tagging	firewall-config		
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
UpdateResolverDnssecConfig	Grants permission to update the DNSSEC validation support status for DNS queries within the specified resource	Write	resolver-dnssec-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey}
firewall-domain-list	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}	aws:ResourceTag/${TagKey}
firewall-config	arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by 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 AWS Route53 Global Resolver

AWS Route53 Global Resolver (service prefix: route53globalresolver) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Route53 Global 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to deliver logs for a global resolver	Permissions management	global-resolver*	aws:ResourceTag/${TagKey}	
AssociateHostedZone	Grants permission to associate a resource to a hosted zone	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateFirewallRule	Grants permission to create multiple firewall rules	Write			
BatchDeleteFirewallRule	Grants permission to delete multiple firewall rules	Write			
BatchUpdateFirewallRule	Grants permission to update multiple firewall rules	Write			
CreateAccessSource	Grants permission to create an access source	Write	dns-view*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccessToken	Grants permission to create an access token	Write	access-token*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDNSView	Grants permission to create a dns view	Write	dns-view*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallDomainList	Grants permission to create a firewall domain list	Write	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Grants permission to create a firewall rule	Write	dns-view*		
			firewall-domain-list		
CreateGlobalResolver	Grants permission to create a global resolver	Write	global-resolver*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessSource	Grants permission to delete an access source	Write	access-source*		
DeleteAccessToken	Grants permission to delete an access token	Write	access-token*		
DeleteDNSView	Grants permission to delete a dns view	Write	dns-view*		
DeleteFirewallDomainList	Grants permission to delete a firewall domain list	Write	firewall-domain-list*		
DeleteFirewallRule	Grants permission to delete a firewall rule	Write			
DeleteGlobalResolver	Grants permission to delete a global resolver	Write	global-resolver*		
DisableDNSView	Grants permission to disable a dns view	Write	dns-view*		
DisassociateHostedZone	Grants permission to disassociate a hosted zone from a resource	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableDNSView	Grants permission to enable a dns view	Write	dns-view*		
GetAccessSource	Grants permission to get an access source	Read	access-source*		
GetAccessToken	Grants permission to get an access token	Read	access-token*		
GetDNSView	Grants permission to get a dns view	Read	dns-view*		
GetFirewallDomainList	Grants permission to get a firewall domain list	Read	firewall-domain-list*		
GetFirewallRule	Grants permission to get a firewall rule	Read			
GetGlobalResolver	Grants permission to get a global resolver	Read	global-resolver*		
GetHostedZoneAssociation	Grants permission to get a hosted zone association	Read			
GetManagedFirewallDomainList	Grants permission to get a managed firewall domain list	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportFirewallDomains	Grants permission to import firewall domains from an S3 bucket	Write	firewall-domain-list*		s3:GetObject s3:ListBucket
ListAccessSources	Grants permission to list access sources	List			
ListAccessTokens	Grants permission to list access tokens	List			
ListDNSViews	Grants permission to list dns views	List			
ListFirewallDomainLists	Grants permission to list firewall domain lists	List			
ListFirewallDomains	Grants permission to list firewall domains	Read	firewall-domain-list*		
ListFirewallRules	Grants permission to list firewall rules	List	dns-view*		
ListGlobalResolvers	Grants permission to list global resolvers	List			
ListHostedZoneAssociations	Grants permission to list hosted zone associations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListManagedFirewallDomainLists	Grants permission to list managed firewall domain lists	List			
ListTagsForResource	Grants permission to list tags for a resource	Write	access-source		
			access-token		
			dns-view		
			firewall-domain-list		
			global-resolver		
TagResource	Grants permission to tag a resource	Tagging	access-source		
			access-token		
			dns-view		
			firewall-domain-list		
			global-resolver		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	access-source		
			access-token		
			dns-view		
			firewall-domain-list		
			global-resolver		
				aws:TagKeys	
UpdateAccessSource	Grants permission to update an access source	Write	access-source*		
UpdateAccessToken	Grants permission to update an access token	Write	access-token*		
UpdateDNSView	Grants permission to update a dns view	Write	dns-view*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFirewallDomains	Grants permission to update firewall domains	Write	firewall-domain-list*		
UpdateFirewallRule	Grants permission to update an firewall rule	Write			
UpdateGlobalResolver	Grants permission to update a global resolver	Write	global-resolver*		
UpdateHostedZoneAssociation	Grants permission to update a hosted zone association	Write			

Resource types defined by AWS Route53 Global 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
access-source	`arn:${Partition}:route53globalresolver::${Account}:access-source/${Id}`	aws:ResourceTag/${TagKey}
access-token	`arn:${Partition}:route53globalresolver::${Account}:access-token/${Id}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
dns-view	arn:${Partition}:route53globalresolver::${Account}:dns-view/${Id}	aws:ResourceTag/${TagKey}
firewall-domain-list	arn:${Partition}:route53globalresolver::${Account}:firewall-domain-list/${Id}	aws:ResourceTag/${TagKey}
global-resolver	arn:${Partition}:route53globalresolver::${Account}:global-resolver/${Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS Route53 Global Resolver

AWS Route53 Global 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for AWS RTB Fabric

AWS RTB Fabric (service prefix: `rtbfabric`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS RTB Fabric

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptLink	Grants permission to accept a link invitation from another Gateway	Write	Link*		
CreateInboundExternalLink	Grants permission to create an inbound external link for a responder gateway	Write	ResponderGateway*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateLink	Grants permission to create a new link between RTB applications	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundExternalLink	Grants permission to create an outbound external link for a requester gateway to connect to external public responder endpoints	Write	RequesterGateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRequesterGateway	Grants permission to create a requester gateway	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResponderGateway	Grants permission to create a responder gateway	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteInboundExternalLink	Grants permission to delete an inbound external link	Write	InboundExternalLink*		
			ResponderGateway*		
DeleteLink	Grants permission to delete a link between RTB applications	Write	Link*		
DeleteOutboundExternalLink	Grants permission to delete an outbound external link	Write	OutboundExternalLink*		
			RequesterGateway*		
DeleteRequesterGateway	Grants permission to delete a requester gateway	Write	RequesterGateway*		
DeleteResponderGateway	Grants permission to delete a responder gateway	Write	ResponderGateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInboundExternalLink	Grants permission to retrieve information about an inbound external link	Read	InboundExternalLink*		
			ResponderGateway*		
GetLink	Grants permission to retrieve information about a link between RTB applications	Read	Link*		
GetOutboundExternalLink	Grants permission to retrieve information about an outbound external link	Read	OutboundExternalLink*		
			RequesterGateway*		
GetRequesterGateway	Grants permission to retrieve information about a requester gateway	Read	RequesterGateway*		
GetResponderGateway	Grants permission to retrieve information about a responder gateway	Read	ResponderGateway*		
ListLinks	Grants permission to list links associated with an RTB application	List			
ListRequesterGateways	Grants permission to list requester gateways with optional filtering and pagination	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResponderGateways	Grants permission to list responder gateways with optional filtering and pagination	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	InboundExternalLink		
			Link		
			OutboundExternalLink		
			RequesterGateway		
			ResponderGateway		
RejectLink	Grants permission to reject a link request between RTB applications	Write	Link*		
TagResource	Grants permission to assign one or more tags (key-value pairs) to the specified resource	Tagging	InboundExternalLink		
			Link		
			OutboundExternalLink		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Requester Gateway		
			Responder Gateway		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag or tags from a resource	Tagging	InboundExternalLink		
			Link		
			OutboundExternalLink		
			Requester Gateway		
			Responder Gateway		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLink	Grants permission to update configuration settings for an existing link	Write	Link*		
UpdateLinkModuleFlow	Grants permission to update a link module flow	Write	Link*		
UpdateRequesterGateway	Grants permission to update a requester gateway	Write	RequesterGateway*		
UpdateResponderGateway	Grants permission to update a responder gateway	Write	ResponderGateway*		

Resource types defined by AWS RTB Fabric

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
InboundExternalLink	`arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}/link/${LinkId}`	aws:ResourceTag/${TagKey} rtbfabric:InboundExternalLinkLinkId

Resource types	ARN	Condition keys
		rtbfabric:RespondergatewayGatewayId
Link	arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}/link/${LinkId}	aws:ResourceTag/${TagKey} rtbfabric:LinkLinkId rtbfabric:RequestergatewayGatewayId rtbfabric:RespondergatewayGatewayId
OutboundExternalLink	arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}/link/${LinkId}	aws:ResourceTag/${TagKey} rtbfabric:OutboundExternalLinkLinkId rtbfabric:RequestergatewayGatewayId
RequesterGateway	arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey} rtbfabric:RequestergatewayGatewayId
ResponderGateway	arn:${Partition}:rtbfabric:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey} rtbfabric:RespondergatewayGatewayId

Condition keys for AWS RTB Fabric

AWS RTB Fabric defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
rtbfabric:InboundExternalLinkGatewayId	Filters access by gateway identifier supporting rtb-gw-* formats	String
rtbfabric:InboundExternalLinkLinkId	Filters access by InboundExternalLink resource linkId identifier	String
rtbfabric:LinkLinkId	Filters access by Link resource linkId identifier	String
rtbfabric:OutboundExternalLinkLinkId	Filters access by OutboundExternalLink resource linkId identifier	String

Condition keys	Description	Type
rtbfabric:RequesterGatewayGatewayId	Filters access by gateway identifier supporting rtb-gw-* formats	String
rtbfabric:ResponderGatewayGatewayId	Filters access by gateway identifier supporting rtb-gw-* formats	String

Actions, resources, and condition keys for Amazon S3

Amazon S3 (service prefix: s3) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon S3
- Resource types defined by Amazon S3
- Condition keys for Amazon S3

Actions defined by Amazon S3

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortMultipartUpload	Grants permission to abort a multipart upload	Write	accesspointobject		
			object		
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion 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	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-metadata-directive	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-server-side-encryption-customer-algorithm s3:x-amz-storage-class s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				website-redirect-location	
CreateAccessGrant	Grants permission to create Access Grant	Permissions management	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateAccessGrantsInstance	Grants permission to Create Access Grants Instance	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessGrantsLocation	Grants permission to create Access Grants location	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:locationconstraint s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256 s3:AccessPointTag/${TagKey} aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAccessPointForObjectLambda	Grants permission to create an object lambda enabled accesspoint	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucket	Grants permission to create a new bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:locationconstraint s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-bucket-namespace s3:x-amz-object-ownership aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucketMetadataTableConfiguration	Grants permission to create a new S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		kms:DescribeKey s3tables:CreateNamespace s3tables:CreateTable s3tables:CreateTableBucket s3tables:GetTable s3tables:PutTableBucketPolicy s3tables:PutTableEncryption s3tables:PutTablePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateJob	Grants permission to create a new Amazon S3 Batch Operations job	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:RequestJobPriority s3:RequestJobOperation aws:TagKeys aws:RequestTag/	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
CreateMultiRegionAccessPoint	Grants permission to create a new Multi-Region Access Point	Write	multiregionaccesspoint*		
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStorageLensGroup	Grants permission to create an Amazon S3 Storage Lens group	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessGrant	Grants permission to delete Access Grant	Permissions management	accessgrant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsInstance	Grants permission to Delete Access Grants Instance	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsInstanceResourcePolicy	Grants permission to read Access grants instance resource policy	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsLocation	Grants permission to delete Access Grants location	Permissions management	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessPoint	Grants permission to delete the access point named in the URI	Write	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteAccessPointForObjectLambda	Grants permission to delete the object lambda enabled access point named in the URI	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccessPointPolicy	Grants permission to delete the policy on a specified access point	Permissions management	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteAccessPointPolicyForObjectLambda	Grants permission to delete the policy on a specified object lambda enabled access point	Permissions management	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBucket	Grants permission to delete the bucket named in the URI	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBucketMetadataTableConfiguration	Grants permission to delete the S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBucketPolicy	Grants permission to delete the policy on a specified bucket	Permissions management	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteBucketWebsite	Grants permission to remove the website configuration for a bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteJobTagging	Grants permission to remove tags from an existing Amazon S3 Batch Operations job	Tagging	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation	
DeleteMultiRegionAccessPoint	Grants permission to delete the Multi-Region Access Point named in the URI	Write	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
DeleteObject	Grants permission to remove the null version of an object and insert a delete marker, which becomes the current version of the object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:if-match	
DeleteObjectTagging	Grants permission to use the tagging subresource to remove the entire tag set from the specified object	Tagging	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteObjectVersion	Grants permission to remove a specific version of an object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
DeleteObjectVersionTagging	Grants permission to remove the entire tag set for a specific version of the object	Tagging	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
DeleteStorageLensConfiguration	Grants permission to delete an existing Amazon S3 Storage Lens configuration	Write	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteStorageLensConfigurationTagging	Grants permission to remove tags from an existing Amazon S3 Storage Lens configuration	Tagging	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteStorageLensGroup	Grants permission to delete an existing S3 Storage Lens group	Write	storagelensgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJob	Grants permission to retrieve the configuration parameters and status for a batch operations job	Read	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DescribeMultiRegionAccessPointOperation	Grants permission to retrieve the configurations for a Multi-Region Access Point	Read	multiregionaccesspointrequestarn*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
DissociateAccessGrantsIdentityCenter	Grants permission to disassociate Access Grants identity center	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccelerateConfiguration	Grants permission to uses the accelerate subresource to return the Transfer Acceleration state of a bucket, which is either Enabled or Suspended	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetAccessGrant	Grants permission to read Access Grant	Read	accessgrant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstance	Grants permission to Read Access Grants Instance	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstanceForPrefix	Grants permission to Read Access Grants Instance by prefix	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstanceResourcePolicy	Grants permission to read Access grants instance resource policy	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsLocation	Grants permission to read Access Grants location	Read	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPoint	Grants permission to return configuration information about the specified access point	Read		s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
GetAccessPointConfigurationForObjectLambda	Grants permission to retrieve the configuration of the object lambda enabled access point	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointForObjectLambda	Grants permission to create an object lambda enabled accesspoint	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointPolicy	Grants permission to return the access point policy associated with the specified access point	Read	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
GetAccessPointPolicyForObjectLambda	Grants permission to return the access point policy associated with the specified object lambda enabled access point	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointPolicyStatus	Grants permission to return the policy status for a specific access point policy	Read	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
GetAccessPointPolicyStatusForObjectLambda	Grants permission to return the policy status for a specific object lambda access point policy	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountPublicAccessBlock	Grants permission to retrieve the PublicAccessBlock configuration for an AWS account	Read		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAnalyticsConfiguration	Grants permission to get an analytics configuration from an Amazon S3 bucket, identified by the analytics configuration ID	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketAbac	Grants permission to retrieve ABAC configuration for a general purpose bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketAcl	Grants permission to use the acl subresource to return the access control list (ACL) of an Amazon S3 bucket	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketCORS	Grants permission to return the CORS configuration information set for an Amazon S3 bucket	Read	accesspoint bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketLocation	Grants permission to return the Region that an Amazon S3 bucket resides in	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketLogging	Grants permission to return the logging status of an Amazon S3 bucket and the permissions users have to view or modify that status	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketMetadataTableConfiguration	Grants permission to return the S3 Metadata configuration for a specified general purpose bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketNotification	Grants permission to get the notification configuration of an Amazon S3 bucket	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketObjectLockConfiguration	Grants permission to get the Object Lock configuration of an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:signatureversion	
GetBucketOwnershipControls	Grants permission to retrieve ownership controls on a bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketPolicy	Grants permission to return the policy of the specified bucket	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketPolicyStatus	Grants permission to retrieve the policy status for a specific Amazon S3 bucket, which indicates whether the bucket is public	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketPublicAccessBlock	Grants permission to retrieve the PublicAccessBlock configuration for an Amazon S3 bucket	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketRequestPayment	Grants permission to return the request payment configuration for an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketTagging	Grants permission to return the tag set associated with an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketVersioning	Grants permission to return the versioning state of an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketWebsite	Grants permission to return the website configuration for an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetDataAccess	Grants permission to get Access	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEncryptionConfiguration	Grants permission to return the default encryption configuration an Amazon S3 bucket	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIntelligentTieringConfiguration	Grants permission to get an or list all Amazon S3 Intelligent Tiering configuration in a S3 Bucket	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInventoryConfiguration	Grants permission to return an inventory configuration from an Amazon S3 bucket, identified by the inventory configuration ID	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetJobTagging	Grants permission to return the tag set of an existing Amazon S3 Batch Operations job	Read	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLifecycleConfiguration	Grants permission to return the lifecycle configuration information set on an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetMetricsConfiguration	Grants permission to get a metrics configuration from an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetMultiRegionAccessPoint	Grants permission to return configuration information about the specified Multi-Region Access Point	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointPolicy	Grants permission to return the access point policy associated with the specified Multi-Region Access Point	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointPolicyStatus	Grants permission to return the policy status for a specific Multi-Region Access Point policy	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointRoutes	Grants permission to return the route configuration for a Multi-Region Access Point	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetObject	Grants permission to retrieve objects from Amazon S3	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectAcl	Grants permission to return the access control list (ACL) of an object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectAttributes	Grants permission to retrieve attributes related to a specific object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectLegalHold	Grants permission to get an object's current Legal Hold status	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectRetention	Grants permission to retrieve the retention settings for an object	Read	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectTagging	Grants permission to return the tag set of an object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectTorrent	Grants permission to return torrent files from an Amazon S3 bucket	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectVersion	Grants permission to retrieve a specific version of an object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionAcl	Grants permission to return the access control list (ACL) of a specific object version	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionAttributes	Grants permission to retrieve attributes related to a specific version of an object	Read	accesspointobject		
			object		
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionForReplication	Grants permission to replicate both unencrypted objects and objects encrypted with SSE-S3 or SSE-KMS	Read	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectVersionTagging	Grants permission to return the tag set for a specific version of the object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionTorrent	Grants permission to get Torrent files about a different version using the versionId subresource	Read	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReplicationConfiguration	Grants permission to get the replication configuration information set on an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensConfiguration	Grants permission to get an Amazon S3 Storage Lens configuration	Read	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensConfigurationTagging	Grants permission to get the tag set of an existing Amazon S3 Storage Lens configuration	Read	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensDashboard	Grants permission to get an Amazon S3 Storage Lens dashboard	Read	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensGroup	Grants permission to get an Amazon S3 Storage Lens group	Read	storagelensgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
InitiateReplication [permission only]	Grants permission to initiate the replication process by setting replication status of an object to pending	Write	object*		
				s3:ResourceAccount	
ListAccessGrants	Grants permission to list Access Grant	List	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessGrantsInstances	Grants permission to List Access Grants Instances	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListAccessGrantsLocations	Grants permission to list Access Grants locations	List	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPoints	Grants permission to list access points	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPointsForObjectLambda	Grants permission to list object lambda enabled accesspoints	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAllMyBuckets	Grants permission to list all buckets owned by the authenticated sender of the request	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	accesspoint bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
	Grants permission to list in-progress multipart uploads	List	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBucketMultipartUploads					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256 s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
ListBucketVersions	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCallerAccessGrants	Grants permission to list caller's Access Grant	List	accessgrantsinstance*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListJobs	Grants permission to list current jobs and jobs that have ended recently	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMultiRegionAccessPoints	Grants permission to list Multi-Region Access Points	List		s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStorageLensConfigurations	Grants permission to list Amazon S3 Storage Lens configurations	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStorageLensGroups	Grants permission to list S3 Storage Lens groups	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListTagsForResource	Grants permission to list the tags attached to the specified resource	List	accessgrant		
			accessgrantsinstance		
			accessgrantslocation		
			accesspoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			bucket		
			storagelensgroup		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ObjectOwnerOverrideToBucketOwner	Grants permission to change replica ownership	Permissions management	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PauseReplication [permission only]	Grants permission to pause S3 Replication from target source buckets to destination buckets	Write	bucket*		s3:GetReplicationConfiguration s3:PutReplicationConfiguration

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:destinationRegion s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccelerateConfiguration	Grants permission to use the accelerate subresource to set the Transfer Acceleration state of an existing S3 bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutAccessGrantsInstanceResourcePolicy	Grants permission to put Access grants instance resource policy	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
PutAccessPointConfigurationForObjectLambda	Grants permission to set the configuration of the object lambda enabled access point	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccessPointPolicy	Grants permission to associate an access policy with a specified access point	Permissions management	accesspoint*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutAccessPointPolicyForObjectLambda	Grants permission to associate an access policy with a specified object lambda enabled access point	Permissions management	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccessPointPublicAccessBlock	Grants permission to associate public access block configurations with a specified access point, while creating a access point	Permissions management			
PutAccountPublicAccessBlock	Grants permission to create or modify the PublicAccessBlock configuration for an AWS account	Permissions management		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAnalyticsConfiguration	Grants permission to set an analytics configuration for the bucket, specified by the analytics configuration ID	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketAbac	Grants permission to set ABAC configuration for a general purpose bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketAcl	Grants permission to set the permissions on an existing bucket using access control lists (ACLs)	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp	
PutBucketCORS	Grants permission to set the CORS configuration for an Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketLogging	Grants permission to set the logging parameters for an Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketNotification	Grants permission to receive notifications when certain events happen in an Amazon S3 bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketObjectLockConfiguration	Grants permission to put Object Lock configuration on a specific bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:TlsVersion s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketOwnershipControls	Grants permission to add, replace or delete ownership controls on a bucket	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketPolicy	Grants permission to add or replace a bucket policy on a bucket	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketPublicAccessBlock	Grants permission to create or modify the PublicAccessBlock configuration for a specific Amazon S3 bucket	Permissions management	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketRequestPayment	Grants permission to set the request payment configuration of a bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketTagging	Grants permission to add a set of tags to an existing Amazon S3 bucket	Tagging	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketVersioning	Grants permission to set the versioning state of an existing Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketWebsite	Grants permission to set the configuration of the website that is specified in the website subresource	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutEncryptionConfiguration	Grants permission to set the encryption configuration for an Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutIntelligentTieringConfiguration	Grants permission to create new or update or delete an existing Amazon S3 Intelligent Tiering configuration	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutInventoryConfiguration	Grants permission to add an inventory configuration to the bucket, identified by the inventory ID	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:InventoryAccessibleOptionalFields	
PutJobTagging	Grants permission to replace tags on an existing Amazon S3 Batch Operations job	Tagging	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
PutLifecycleConfiguration	Grants permission to create a new lifecycle configuration for the bucket or replace an existing lifecycle configuration	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricsConfiguration	Grants permission to set or update a metrics configuration for the CloudWatch request metrics from an Amazon S3 bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutMultiRegionAccessPointPolicy	Grants permission to associate an access policy with a specified Multi-Region Access Point	Permissions management	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
PutObject	Grants permission to add an object to a bucket	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256 s3:x-amz-copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-metadata-directive s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-server-side-encryption-customer-algorithm s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				storage-class s3:x-amz-website-redirect-location s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-retention-days s3:object-lock-legal-hold s3:if-match s3:if-none-match	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ObjectCreationOperation	
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket	Permissions management	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-storage-class	
PutObjectLegalHold	Grants permission to apply a Legal Hold configuration to the specified object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:object-lock-legal-hold	
PutObjectRetention	Grants permission to place an Object Retention configuration on an object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-re	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tention-days	
PutObjectTagging	Grants permission to set the supplied tag-set to an object that already exists in a bucket	Tagging	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectVersionAcl	Grants permission to use the acl subresource to set the access control list (ACL) permissions for an object that already exists in a bucket	Permissions management	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-acl s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-storage-class	
PutObjectVersionTagging	Grants permission to set the supplied tag-set for a specific version of an object	Tagging	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
PutReplicationConfiguration	Grants permission to create a new replication configuration or replace an existing one	Write	bucket*		iam:PassRole
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:isReplicationPauseRequest	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutStorageLensConfiguration	Grants permission to create or update an Amazon S3 Storage Lens configuration	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
PutStorageLensConfigurationTagging	Grants permission to put or replace tags on an existing Amazon S3 Storage Lens configuration	Tagging	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
Replicate Delete	Grants permission to replicate delete markers to the destination bucket	Write	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
Replicate Object	Grants permission to replicate objects and object tags to the destination bucket	Write	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms-key-id s3:x-amz-server-side-encryption-customer-algorithm	
Replicate Tags	Grants permission to replicate object tags to the destination bucket	Tagging	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
RestoreObject	Grants permission to restore an archived copy of an object back into Amazon S3	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
SubmitMultiRegionAccessPointRoutes	Grants permission to submit a route configuration update for a Multi-Region Access Point	Write	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
TagResource	Grants permission to add tags to the specified resource	Tagging	accessgrant		
			accessgrantsinstance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			accessgrantslocation		
			accesspoint		
			bucket		
			storagelensgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	accessgrant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			accessgrantsinstance		
			accessgrantslocation		
			accesspoint		
			bucket		
			storagelensgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys	
UpdateAccessGrantsLocation	Grants permission to update Access Grants location	Permissions management	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBucketMetadataInventoryTableConfiguration	Grants permission to update the inventory table configuration on an existing S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		kms:DescribeKey s3tables:CreateNamespace s3tables:CreateTable s3tables:CreateTableBucket s3tables:GetTable s3tables:PutTableEncryption s3tables:PutTablePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBucketMetadataJournalTableConfiguration	Grants permission to update the journal table configuration on an existing S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
UpdateJobPriority	Grants permission to update the priority of an existing job	Write	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:RequestJobPriority s3:ExistingJobPriority s3:ExistingJobOperation	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateJobStatus	Grants permission to update the status for the specified job	Write	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation s3:JobSuspendedCause	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateObjectEncryption	Grants permission to update the server-side encryption type of an existing object in a general purpose bucket	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3: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	
UpdateStorageLensGroup	Grants permission to update an existing S3 Storage Lens group	Write	storagelensgroup*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Resource types defined by Amazon S3

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
accesspoint	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}	aws:ResourceTag/${TagKey} s3:AccessPointNetworkOrigin s3:AccessPointTag/${TagKey} s3:DataAccessPointAccount s3:DataAccessPointArn
accesspointobject	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}/object/${ObjectName}	aws:ResourceTag/${TagKey} s3:AccessPointNetworkOrigin s3:AccessPointTag/${TagKey} s3:BucketTag/${TagKey} s3:DataAccessPointAccount s3:DataAccessPointArn
bucket	arn:${Partition}:s3:::${BucketName}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		s3:BucketTag/${TagKey}
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}	aws:ResourceTag/${TagKey} s3:BucketTag/${TagKey}
job	arn:${Partition}:s3:${Region}:${Account}:job/${JobId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
storagelensconfiguration	arn:${Partition}:s3:${Region}:${Account}:storage-lens/${ConfigId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
storagelensgroup	arn:${Partition}:s3:${Region}:${Account}:storage-lens-group/${Name}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
objectlambdaaccesspoint	arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}	

Resource types	ARN	Condition keys
multiregionaccesspoint	arn:${Partition}:s3::${Account}:accesspoint/${AccessPointAlias}	
multiregionaccesspointrequestarn	arn:${Partition}:s3:us-west-2:${Account}:async-request/mrap/${Operation}/${Token}	
accessgrantsinstance	arn:${Partition}:s3:${Region}:${Account}:access-grants/default	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
accessgrantslocation	arn:${Partition}:s3:${Region}:${Account}:access-grants/default/location/${Token}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
accessgrant	arn:${Partition}:s3:${Region}:${Account}:access-grants/default/grant/${Token}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Condition keys for Amazon S3

Amazon S3 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
s3:AccessGrantScope	Filters access by the grant scope of access grants grant	String
s3:AccessGrantsInstanceArn	Filters access by access grants instance ARN	ARN
s3:AccessGrantsLocationScope	Filters access by the location scope of access grants location	String
s3:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String
s3:AccessPointTag/${TagKey}	Filters access by existing access point tag key and value	String

Condition keys	Description	Type
s3:BucketTag/${TagKey}	Filters access by the tags associated with the bucket	String
s3:DataAccessPointAccount	Filters access by the AWS Account ID that owns the access point	String
s3:DataAccessPointArn	Filters access by an access point Amazon Resource Name (ARN)	ARN
s3:ExistingJobOperation	Filters access by operation to updating the job priority	String
s3:ExistingJobPriority	Filters access by priority range to cancelling existing jobs	Numeric
s3:ExistingObjectTag/<key>	Filters access by existing object tag key and value	String
s3:InventoryAccessibleOptionalFields	Filters access by restricting which optional metadata fields a user can add when configuring S3 Inventory reports	ArrayOfString
s3:JobSuspendedCause	Filters access by a specific job suspended cause (for example, AWAITING_CONFIRMATION) to cancelling suspended jobs	String
s3:ObjectCreationOperation	Filters access by whether or not the operation creates an object	Bool
s3:RequestJobOperation	Filters access by operation to creating jobs	String

Condition keys	Description	Type
s3:RequestJobPriority	Filters access by priority range to creating new jobs	Numeric
s3:RequestObjectTag/<key>	Filters access by the tag keys and values to be added to objects	String
s3:RequestObjectTagKeys	Filters access by the tag keys to be added to objects	ArrayOfString
s3:ResourceAccount	Filters access by the resource owner AWS account ID	String
s3:TlsVersion	Filters access by the TLS version used by the client	Numeric
s3:authType	Filters access by authentication method	String
s3:delimiter	Filters access by delimiter parameter	String
s3:destinationRegion	Filters access by a specific replication destination region for targeted buckets of the AWS FIS action aws:s3:bucket-pause-replication	String
s3:if-match	Filters access by the request's 'If-Match' conditional header	String
s3:if-none-match	Filters access by the request's 'If-None-Match' conditional header	String
s3:isReplicationPauseRequest	Filters access by request made via AWS FIS action aws:s3:bucket-pause-replication	Bool
s3:locationconstraint	Filters access by a specific Region	String
s3:max-keys	Filters access by maximum number of keys returned in a ListBucket request	Numeric

Condition keys	Description	Type
s3:object-lock-legal-hold	Filters access by object legal hold status	String
s3:object-lock-mode	Filters access by object retention mode (COMPLIANCE or GOVERNANCE)	String
s3:object-lock-remaining-retention-days	Filters access by remaining object retention days	Numeric
s3:object-lock-retain-until-date	Filters access by object retain-until date	Date
s3:prefix	Filters access by key name prefix	String
s3:signatureAge	Filters access by the age in milliseconds of the request signature	Numeric
s3:signatureversion	Filters access by the version of AWS Signature used on the request	String
s3:versionid	Filters access by a specific object version	String
s3:x-amz-acl	Filters access by canned ACL in the request's x-amz-acl header	String
s3:x-amz-bucket-namespace	Filters access by general purpose bucket namespace type	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

Condition keys	Description	Type
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
s3:x-amz-object-ownership	Filters access by Object Ownership	String
s3:x-amz-server-side-encryption	Filters access by server-side encryption	String
s3:x-amz-server-side-encryption-aws-kms-key-id	Filters access by AWS KMS customer managed CMK for server-side encryption	ARN
s3:x-amz-server-side-encryption-customer-algorithm	Filters access by customer specified algorithm for server-side encryption	String
s3:x-amz-storage-class	Filters access by storage class	String

Condition keys	Description	Type
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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
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 aws:RequestTag/${TagKey} aws:TagKeys	

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, etc	Write	bucket*		
			accesspoint	s3express:Permissions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:authType s3express:ResourceAccount s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-encryption	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:x-amz-server-side-encryption-aws-kms-key-id s3express:AllAccessRestrictedToLocalZoneGroup s3express:Permissions	
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	
GetAccessPoint	Grants permission to return configuration information about 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	
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:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
ListTagsForResource	Grants permission to lists all of the tags for a specified resource	List	accesspoint 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	
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
				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	
TagResource	Grants permission to create a new user-defined tag or update an existing tag	Tagging	accesspoint		
			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 aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the specified user-defined tags from an S3 resource	Tagging	accesspoint		
			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 aws:TagKeys	

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}	aws:ResourceTag/${TagKey} s3express:BucketTag/${TagKey}
accesspoint	arn:${Partition}:s3express:${Region}:${Account}:accesspoint/${AccessPointName}	aws:ResourceTag/${TagKey} s3express:AccessPointTag/${TagKey}

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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Condition keys	Description	Type
s3express:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String
s3express:AccessPointTag/${TagKey}	Filters access by tag key-value pairs attached to the access point	String
s3express:AllAccessRestrictedToLocalZoneGroup	Filters access by AWS Local Zone network border group(s) provided in this condition key	String
s3express:BucketTag/${TagKey}	Filters access by tag key-value pairs attached to the bucket	String
s3express:DataAccessPointAccount	Filters access by the AWS Account ID that owns the access point	String
s3express:DataAccessPointArn	Filters access by an access point Amazon Resource Name (ARN)	ARN
s3express:LocationName	Filters access by a specific Availability Zone or Local 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 AWS account ID	String

Condition keys	Description	Type
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 AWS 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
s3express:x-amz-server-side-encryption-aws-kms-key-id	Filters access by AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortMultipartUpload	Grants permission to abort a multipart upload 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*		
AddTagsToVault	Grants permission to add the specified tags to a vault	Tagging	vault*		
CompleteMultipartUpload	Grants permission to complete a multipart upload process	Write	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ListProvisionedCapacity	Grants permission to list the provisioned capacity for the specified AWS 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 AWS account	Write			
RemoveTagsFromVault	Grants permission to remove one or more tags from the set of tags attached to a vault	Tagging	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 AWS global condition context keys.

Condition keys	Description	Type
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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortMultipartUpload	Grants permission to abort a multipart upload	Write	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-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:authType s3-object-lambda:signatureAge 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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteObjectVersion	Grants permission to remove a specific version of an object	Write	objectlambdaaccesspoint*		
				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 AWS 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 S3 on Outposts

Amazon S3 on Outposts (service prefix: `s3-outposts`) 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 on Outposts

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortMultipartUpload	Grants permission to abort a multipart upload	Write	object*		
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outpos	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-content-sha256	
CreateBucket	Grants permission to create a new bucket	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
CreateEndpoint	Grants permission to create a new endpoint	Write	endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-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
				s3-outposts:DataAccessPointArn s3-outposts:DataAccessPointAccount s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-content-sha256	
DeleteBucket	Grants permission to delete the bucket named in the URI	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
DeleteEndpoint	Grants permission to delete the endpoint named in the URI	Write	endpoint*		

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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteObjectTagging	Grants permission to use the tagging subresource to remove the entire tag set from the specified object	Tagging	object*		
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:versionid s3-outposts: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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts: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		s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-content-sha256	
GetAccessPointPolicy	Grants permission to returns the access point policy associated with the specified access point	Read	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-content-sha256	
GetBucket	Grants permission to return the bucket configuration associated with an Amazon S3 bucket	Read	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
GetObject	Grants permission to retrieve objects from Amazon S3	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:signatureversion s3-outposts: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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionForReplication	Grants permission to replicate both unencrypted objects and objects encrypted with SSE-KMS	Read	object*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outposts:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:signatureversion s3-outposts:versionid s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPoints	Grants permission to list access points	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	accesspoint* bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outposts:max-keys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListBucketMultipartUploads	Grants permission to list in-progress multipart uploads	List	accesspoint* bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBucketVersions	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	bucket*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:delimiter s3-outpos	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ts:max-keys s3-outposts:prefix s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
ListEndpoints	Grants permission to list endpoints	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signat	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ureversion s3-outposts:x-amz-content-sha256	
ListOutpostsWithS3	Grants permission to list outposts with S3 capacity	List			
ListRegionalBuckets	Grants permission to list all buckets owned by the authenticated sender of the request	List		s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSharedEndpoints	Grants permission to list shared endpoints	List			
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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:x-amz-content-sha256	
PutBucketPolicy	Grants permission to add or replace a bucket policy on a bucket	Permissions management	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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 bucket or replace an existing lifecycle configuration	Write	bucket*		
				s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
PutObject	Grants permission to add an object to a bucket	Write	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:RequestObjectTag/<key> s3-outposts:RequestObjectTagKeys s3-outpos	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-copy-source s3-outposts:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				metadata-directive s3-outposts:x-amz-server-side-encryption s3-outposts:x-amz-storage-class	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for an object that already exists in a bucket	Permissions management	object*	s3-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:authType s3-outpos	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-acl s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-storage-class	
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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key> s3-outposts:Reques	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
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-outposts:DataAccessPointAccount s3-outposts:DataAccessPointArn s3-outposts:AccessPointNetworkOrigin s3-outposts:ExistingObjectTag/<key> s3-outposts:RequestObjectTag/<key> s3-outposts:Reques	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tObjectTagKeys s3-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:versionid s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	
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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts: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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256 s3-outposts:x-amz-server-side-encryption	
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-outposts:authType s3-outposts:signatureAge s3-outposts:signatureversion s3-outposts:x-amz-content-sha256	

Resource types defined by Amazon S3 on Outposts

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:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/accesspoint/${AccessPointName}	
bucket	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}	
endpoint	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/endpoint/${EndpointId}	
object	arn:${Partition}:s3-outposts:${Region}:${Account}:outpost/${OutpostId}/bucket/${BucketName}/object/${ObjectName}	

Condition keys for Amazon S3 on Outposts

Amazon S3 on Outposts defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
s3-outposts:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String

Condition keys	Description	Type
s3-outposts:DataAccessPointAccount	Filters access by the AWS Account ID that owns the access point	String
s3-outposts:DataAccessPointArn	Filters access by an access point Amazon Resource Name (ARN)	ARN
s3-outposts:ExistingObjectTag/<key>	Filters access by requiring that an existing object tag has a specific tag key and value	String
s3-outposts:RequestObjectTag/<key>	Filters access by restricting the tag keys and values allowed on objects	String
s3-outposts:RequestObjectTagKeys	Filters access by restricting the tag keys allowed on objects	String
s3-outposts:authType	Filters access by restricting incoming requests to a specific authentication method	String
s3-outposts:delimiter	Filters access by requiring the delimiter parameter	String
s3-outposts:max-keys	Filters access by limiting the maximum number of keys returned in a ListBucket request	Numeric
s3-outposts:prefix	Filters access by key name prefix	String

Condition keys	Description	Type
s3-outposts:signatureAge	Filters access by identifying the length of time, in milliseconds, that a signature is valid in an authenticated request	Numeric
s3-outposts:signatureversion	Filters access by identifying the version of AWS Signature that is supported for authenticated requests	String
s3-outposts:versionid	Filters access by a specific object version	String
s3-outposts:x-amz-acl	Filters access by requiring the x-amz-acl header with a specific canned ACL in a request	String
s3-outposts:x-amz-content-sha256	Filters access by disallowing unsigned content in your bucket	String
s3-outposts:x-amz-copy-source	Filters access by restricting the copy source to a specific bucket, prefix, or object	String
s3-outposts:x-amz-metadata-directive	Filters access by enabling enforcement of object metadata behavior (COPY or REPLACE) when objects are copied	String
s3-outposts:x-amz-server-side-encryption	Filters access by requiring server-side encryption	String
s3-outposts:x-amz-storage-class	Filters access by storage class	String

Actions, resources, and condition keys for Amazon S3 Tables

Amazon S3 Tables (service prefix: `s3tables`) 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 Tables

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNamespace	Grants permission to create a namespace	Write	TableBucket*		
CreateTable	Grants permission to create a table	Write	TableBucket*		
				s3tables:namespace	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3tables:SSEAlgorithm s3tables:KMSKeyArn s3tables:TableBucketTag/${TagKey} aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTableBucket	Grants permission to create a table bucket	Write	TableBucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3tables:SSEAlgorithm s3tables:KMSKeyArn s3tables:TableBucketTag/${TagKey} aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteNamespace	Grants permission to delete a namespace	Write	TableBucket*		
				s3tables:namespace	
DeleteTable	Grants permission to delete a table	Write	Table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3tables:namespace s3tables:tableName	
DeleteTableBucket	Grants permission to delete a table bucket	Write	TableBucket*		
DeleteTableBucketEncryption	Grants permission to delete encryption configuration on a table bucket	Write	TableBucket*		
DeleteTableBucketMetricsConfiguration	Grants permission to delete a metrics configuration on a table bucket	Write	TableBucket*		
DeleteTableBucketPolicy	Grants permission to delete a policy on a table bucket	Permissions management	TableBucket*		
DeleteTableBucketReplication	Grants permission to delete table bucket replication configuration on a bucket	Write	TableBucket*		
DeleteTablePolicy	Grants permission to delete a policy on a table	Permissions management	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTableReplication	Grants permission to delete table replication configuration on a table	Write	Table*		
				s3tables:namespace s3tables:tableName	
GetNamespace	Grants permission to get a namespace	Read	TableBucket*		
				s3tables:namespace	
GetTable	Grants permission to retrieve a table	Read	Table*		
				s3tables:namespace s3tables:tableName	
GetTableBucket	Grants permission to retrieve a table bucket	Read	TableBucket*		
GetTableBucketEncryption	Grants permission to retrieve encryption configuration on a table bucket	Read	TableBucket*		
GetTableBucketMaintenanceConfiguration	Grants permission to retrieve a maintenance configuration on a table bucket	Read	TableBucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTableBucketMetricsConfiguration	Grants permission to retrieve a metrics configuration on a bucket	Read	TableBucket*		
GetTableBucketPolicy	Grants permission to retrieve a policy on a table bucket	Read	TableBucket*		
GetTableBucketReplication	Grants permission to retrieve a table bucket replication configuration on a bucket	Read	TableBucket*		
GetTableBucketStorageClass	Grants permission to retrieve the storage class configuration for a table bucket	Read	TableBucket*		
GetTableData [permission only]	Grants permission to read metadata and data objects from a table storage endpoint using S3 APIs	Read	Table*		
				s3tables:namespace s3tables:tableName	
GetTableEncryption	Grants permission to retrieve encryption configuration on a table	Read	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTableMaintenanceConfiguration	Grants permission to retrieve a maintenance configuration on a table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTableMaintenanceJobStatus	Grants permission to retrieve the status of maintenance jobs on a table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTableMetadataLocation	Grants permission to retrieve the metadata location of a table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTablePolicy	Grants permission to retrieve a policy on a table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTableRecordExpirationConfiguration	Grants permission to retrieve a table maintenance configuration on a system table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTableRecordExpirationJobStatus	Grants permission to retrieve the status of table record expiration jobs on a system table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTableReplication	Grants permission to retrieve a table replication configuration on a table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTableReplicationStatus	Grants permission to retrieve a table replication status on a table	Read	Table*		
				s3tables:namespace	
				s3tables:tableName	
GetTableStorageClass	Grants permission to retrieve the storage class configuration for a specific table	Read	Table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3tables:namespace s3tables:tableName	
ListNamespaces	Grants permission to list namespaces	List	TableBucket*		
ListTableBuckets	Grants permission to list table buckets	List			
ListTables	Grants permission to list tables	List	TableBucket*		
				s3tables:namespace	
ListTagsForResource	Grants permission to list the tags for an S3 Tables resource	List	Table		
			TableBucket		
				aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTableBucketEncryption	Grants permission to put or overwrite encryption configuration on a table bucket	Write	TableBucket*		
				s3tables:KMSKeyArn s3tables:SSEAlgorithm	
PutTableBucketMaintenanceConfiguration	Grants permission to put a maintenance configuration on a table bucket	Write	TableBucket*		
PutTableBucketMetricsConfiguration	Grants permission to create or overwrite a metrics configuration on a table bucket	Write	TableBucket*		
PutTableBucketPolicy	Grants permission to create or overwrite a policy on a table bucket	Permissions management	TableBucket*		
PutTableBucketReplication	Grants permission to put table bucket replication configuration on a bucket	Write	TableBucket*		
PutTableBucketStorageClass	Grants permission to set or update the storage class configuration for a table bucket	Write	TableBucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3tables:StorageClass	
PutTableData [permission only]	Grants permission to write metadata and data objects to a table storage endpoint using S3 APIs	Write	Table*		
				s3tables:namespace s3tables:tableName	
PutTableEncryption [permission only]	Grants permission to put encryption configuration on a table	Write	Table*		
				s3tables:namespace s3tables:SSEAlgorithm s3tables:KMSKeyArn	
PutTableMaintenanceConfiguration	Grants permission to put a maintenance configuration on a table	Write	Table*		
				s3tables:namespace s3tables:tableName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTablePolicy	Grants permission to create or overwrite a policy on a table	Permissions management	Table*		
				s3tables:namespace s3tables:tableName	
PutTableRecordExpirationConfiguration	Grants permission to put a table record expiration configuration on a system table	Write	Table*		
				s3tables:namespace s3tables:tableName	
PutTableReplication	Grants permission to put table replication configuration on a table	Write	Table*		
				s3tables:namespace s3tables:tableName	
PutTableStorageClass	Grants permission to set or update the storage class configuration for a table	Write	Table*		
				s3tables:namespace s3tables:tableName s3tables:StorageClass	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RenameTable	Grants permission to rename a table or move a table across namespaces	Write	Table*		
				s3tables:namespace s3tables:tableName	
TagResource	Grants permission to tag a S3 Tables resource	Tagging	Table		
			TableBucket		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}	
UntagResource	Grants permission to untag a S3 Tables resource	Tagging	Table		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			TableBucket		
				aws:TagKeys aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}	
UpdateTableMetadataLocation	Grants permission to update the metadata location of a table	Write	Table*		
				s3tables:namespace s3tables:tableName	

Resource types defined by Amazon S3 Tables

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
TableBucket	arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}	aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey}
Table	arn:${Partition}:s3tables:${Region}:${Account}:bucket/${TableBucketName}/table/${TableID}	aws:ResourceTag/${TagKey} s3tables:TableBucketTag/${TagKey} s3tables:namespace s3tables:tableName

Condition keys for Amazon S3 Tables

Amazon S3 Tables defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
s3tables:KMSKeyArn	Filters access by the AWS KMS key ARN for the key used to encrypt a table	ARN
s3tables:SSEAlgorithm	Filters access by the server-side encryption algorithm used to encrypt a table	String
s3tables:StorageClass	Filters access by the storage class that can be set on tables under a table bucket	String
s3tables:TableBucketTag/${TagKey}	Filters access by the tags associated with the table bucket	String
s3tables:namespace	Filters access by the namespaces created in the table bucket	String
s3tables:tableName	Filters access by the name of the tables in the table bucket	String

Actions, resources, and condition keys for Amazon S3 Vectors

Amazon S3 Vectors (service prefix: `s3vectors`) 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 Vectors

- Resource types defined by Amazon S3 Vectors
- Condition keys for Amazon S3 Vectors

Actions defined by Amazon S3 Vectors

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIndex	Grants permission to create a new vector index within a specified vector bucket	Write	Index*		
				s3vectors:sseType s3vectors:kmsKeyArn aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cketTag/${TagKey}	
CreateVectorBucket	Grants permission to create a new vector bucket	Write	VectorBucket*		
				s3vectors:sseType s3vectors:kmsKeyArn aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIndex	Grants permission to delete a specified vector index	Write	Index*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
DeleteVectorBucket	Grants permission to delete a specified vector bucket	Write	VectorBucket*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
DeleteVectorBucketPolicy	Grants permission to delete the IAM resource policy from a specified vector bucket	Permissions management	VectorBucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
DeleteVectors	Grants permission to delete a batch of vectors from a specified vector index	Write	Index*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetIndex	Grants permission to get the attributes of a specified vector index	Read	Index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetVectorBucket	Grants permission to get the attributes of a specified vector bucket	Read	VectorBucket*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetVectorBucketPolicy	Grants permission to get the IAM resource policy for a specific vector bucket	Read	VectorBucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
GetVectors	Grants permission to get a batch of vectors by their vector keys	Read	Index*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
ListIndexes	Grants permission to get a paginated list of all indexes in a specified vector bucket	List	VectorBucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
ListTagsForResource	Grants permission to list tags for specified S3Vector resource	List	Index		
			VectorBucket		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
ListVectorBuckets	Grants permission to get a paginated list of all vector buckets in the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVectors	Grants permission to get a paginated list of all vectors in a specified vector index	List	Index*		s3vectors:GetVectors
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
PutVectorBucketPolicy	Grants permission to add an IAM resource policy to a specified vector bucket	Permissions management	VectorBucket*		
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
PutVectors	Grants permission to add a batch of vectors to a specified vector index	Write	Index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
QueryVectors	Grants permission to find approximate nearest neighbors within a specified search vector index for a given query vector	Read	Index*		s3vectors:GetVectors
				aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
TagResource	Grants permission to tag a S3Vector resource	Tagging	Index		
			VectorBucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	
UntagResource	Grants permission to untag a S3Vector resource	Tagging	Index VectorBucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}	

Resource types defined by Amazon S3 Vectors

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:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}/index/${IndexName}`	aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}

Resource types	ARN	Condition keys
VectorBucket	arn:${Partition}:s3vectors:${Region}:${Account}:bucket/${BucketName}	aws:ResourceTag/${TagKey} s3vectors:VectorBucketTag/${TagKey}

Condition keys for Amazon S3 Vectors

Amazon S3 Vectors defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
s3vectors:VectorBucketTag/${TagKey}	Filters access by the tags associated with the vector bucket	String
s3vectors:kmsKeyArn	Filters access by the AWS KMS key ARN for the key used to encrypt a vector bucket	ARN

Condition keys	Description	Type
s3vectors:sseType	Filters access by server-side encryption type	String

Actions, resources, and condition keys for Amazon SageMaker

Amazon SageMaker (service prefix: `sagemaker`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon SageMaker
- Resource types defined by Amazon SageMaker
- Condition keys for Amazon SageMaker

Actions defined by Amazon SageMaker

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAssociation	Grants permission to associate a lineage entity (artifact, context, action,	Write	action*		
			artifact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	experiment, experiment-trial-component) to each other		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		
			cluster-scheduler-config		
			code-repository		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			compilation-job		
			compute-quota		
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		
			flow-definition		
			hub		
			hub-content		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			inference-component		
			inference-recommendations-job		
			labeling-job		
			mlflow-app		
			mlflow-tracking-server		
			model		
			model-bias-job-definition		
			model-card		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-explainability-job-definition		
			model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
			model-package-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			notebook-instance-lifecycle-config		
			optimization-job		
			partner-app		
			pipeline		
			processing-job		
			project		
			reserved-capacity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			space		
			studio-lifecycle-config		
			training-job		
			training-plan		
			transform-job		
			user-profile		
			workteam		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:TaggingAction	
AssociateTrialComponent	Grants permission to associate a trial component with a trial	Write	experiment-trial*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			experiment-trial-component*		
AttachClusterNodeVolume	Grants permission to attach an Amazon EBS volume to a SageMaker HyperPod cluster node	Write	cluster*		ec2:AttachVolume ec2:DescribeVolumes eks:DescribeCluster
BatchAddClusterNodes	Grants permission to add multiple nodes at a time to a SageMaker HyperPod cluster	Write	cluster*		eks:DescribeCluster
BatchDeleteClusterNodes	Grants permission to batch delete SageMaker HyperPod cluster nodes	Write	cluster*		eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDescribeModelPackage	Grants permission to describe one or more ModelPackages	Read	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
BatchGetMetrics	Grants permission to retrieve metrics associated with SageMaker Resources such as Training Jobs or Trial Components	Read	experiment-trial-component*		
			training-job*		
BatchGetRecord	Grants permission to get a batch of records from one or more feature groups	Read	feature-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchPutMetrics	Grants permission to publish metrics associated with a SageMaker Resource such as a Training Job or Trial Component	Write	experiment-trial-component*		
			training-job*		
CallMlflowAppApi	Grants permission to invoke MLflow APIs	Write	mlflow-app*		
CallPartnerAppApi	Grants permission for Partner App SDK to access the Partner App for reading or writing data use cases	Write	partner-app*		
CreateAction	Grants permission to create an action	Write	action*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAlgorithm	Grants permission to create an algorithm	Write	algorithm*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApp	Grants permission to create an App for a SageMaker UserProfile or Space	Write	app*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType sagemaker:StudioLifecycleConfigArns	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppImageConfig	Grants permission to create an AppImageConfig	Write	app-image-config*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArtifact	Grants permission to create an artifact	Write	artifact*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutoMLJob	Grants permission to create an AutoML job	Write	automl-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InterContainerTrafficEncryption sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutoMLJobV2	Grants permission to create a V2 AutoML job	Write	automl-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InterContainerTrafficEncryption sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a SageMaker HyperPod cluster	Write	cluster*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyImageAttribute ec2:ModifySnapshotAttribute eks:AssociateAccessPolicy eks:CreateAccessEntry eks:DeleteAccessEntry eks:DescribeAccessEntry eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole iam:PassRole sagemaker:AddTags
			reserved-capacity		
			training-plan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClusterSchedulerConfig	Grants permission to create a cluster scheduler config	Write	cluster*		eks:AssociateAccessPolicy eks:DescribeCluster eks:ListAssociatedAccessPolicies sagemaker:AddTags sagemaker:DescribeCluster
			cluster-scheduler-config*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCodeRepository	Grants permission to create a CodeRepository	Write	code-repository*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCompilationJob	Grants permission to create a compilation job	Write	compilation-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateComputeQuota	Grants permission to create a compute quota	Write	cluster*		eks:AssociateAccessPolicy eks:DescribeCluster eks:ListAssociatedAccessPolicies sagemaker:AddTags sagemaker:DescribeCluster
			compute-quota*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateContext	Grants permission to create a context	Write	context*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityJobDefinition	Grants permission to create a data quality job definition	Write	data-quality-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateDeviceFleet	Grants permission to create a device fleet	Write	device-fleet*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Grants permission to create a Domain for SageMaker Studio	Write	domain*		iam:CreateServiceLinkedRole iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AppNetworkAccessType sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:DomainSharingOutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:StudioLifecycleConfigArns	
CreateEdgeDeploymentPlan	Grants permission to create an edge deployment plan	Write	edge-deployment-plan*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEdgeDeploymentStage	Grants permission to create an edge deployment stage	Write	edge-deployment-plan*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEdgePackagingJob	Grants permission to create an edge packaging job	Write	edge-packaging-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEndpoint	Grants permission to create an endpoint using the endpoint configuration specified in the request	Write	endpoint*		sagemaker:AddTags
			endpoint-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEndpointConfig	Grants permission to create an endpoint configuration that can be deployed using Amazon SageMaker hosting services	Write	endpoint-config*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AcceleratorTypes sagemaker:InstanceTypes sagemaker:ModelArn sagemaker:VolumeKmsKey sagemaker:ServerlessMaxConcurrency sagemaker:ServerlessMemorySize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:NetworkIsolation sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateExperiment	Grants permission to create an experiment	Write	experiment*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeatureGroup	Grants permission to create a feature group	Write	feature-group*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FeatureGroupOnlineStoreKmsKey sagemaker:FeatureGroupOfflineStoreKmsKey sagemaker:FeatureGroupOfflineStoreS3Uri sagemaker:FeatureGroupEnableOnlineStore	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:FeatureGroupOfflineStoreConfig sagemaker:FeatureGroupDisableGlueTableCreation	
CreateFlowDefinition	Grants permission to create a flow definition, which defines settings for a human workflow	Write	flow-definition*		iam:PassRole sagemaker:AddTags
				sagemaker:WorkteamArn sagemaker:WorkteamType aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHub	Grants permission to create a hub	Write	hub*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHubContentPresignedUrls	Grants permission to generate S3 presigned URLs with GetObject permission for accessing model artifacts	Read	hub*		
			hub-content*		
CreateHubContentReference	Grants permission to create hub content reference	Write	hub*		sagemaker:AddTags
			hub-content*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHumanTaskUi	Grants permission to define the settings you will use for the human review workflow user interface	Write	human-task-ui*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHyperParameterTuningJob	Grants permission to create a hyper parameter tuning job that can be deployed using Amazon SageMaker	Write	hyper-parameter-tuning-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FileSystemAccessMode sagemaker:FileSystemDirectoryPath sagemaker:FileSystemId sagemaker:FileSystemType sagemaker:InstanceTypes sagemaker:InterContainerTra	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateImage	Grants permission to create a SageMaker Image	Write	image*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageVersion	Grants permission to create a SageMaker ImageVersion	Write	image*		
CreateInferenceComponent	Grants permission to create an inference component on an endpoint	Write	endpoint*		sagemaker:AddTags
			inference-component*		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:ModelArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInferenceExperiment	Grants permission to create an inference experiment	Write	inference-experiment*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceRecommendationsJob	Grants permission to create an inference recommend ations job	Write	inference-recommendations-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabelingJob	Grants permission to start a labeling job. A labeling job takes unlabeled data in and produces labeled data as output, which can be used for training SageMaker models	Write	labeling-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:WorkteamArn sagemaker:WorkteamType sagemaker:VolumeKmsKey sagemaker:OutputKmsKey aws:RequestTag/${TagKey} aws:TagKeys	
CreateLineageGroupPolicy	Grants permission to create a lineage group policy	Write			
CreateMlflowApp	Grants permission to create an MLflow app	Write	mlflow-app*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMlflowTrackingServer	Grants permission to create an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Grants permission to create a model in Amazon SageMaker. In the request, you specify a name for the model and describe one or more containers	Write	model*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:NetworkIsolation sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:DirectGatedModelAccess	
CreateModelBiasJobDefinition	Grants permission to create a model bias job definition	Write	model-bias-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelCard	Grants permission to create a model card	Write	model-card*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCardExportJob	Grants permission to create an export job for a model card	Write	model-card*		
CreateModelExplainabilityJobDefinition	Grants permission to create a model explainability job definition	Write	model-explainability-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelPackage	Grants permission to create a ModelPackage	Write	model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	sagemaker:AddTags
			model-package-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:ModelApprovalStatus sagemaker:CustomerMetadataProperties/${MetadataKey} sagemaker:ModelLifeCycle:Stage sagemaker:ModelLifeCycle:StageStatus	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateModelPackageGroup	Grants permission to create a ModelPackageGroup	Write	model-package-group*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelQualityJobDefinition	Grants permission to create a model quality job definition	Write	model-quality-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateMonitoringSchedule	Grants permission to create a monitoring schedule	Write	monitoring-schedule*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateNotebookInstance	Grants permission to create an Amazon SageMaker notebook instance. A notebook instance is an Amazon EC2 instance running on a Jupyter Notebook	Write	notebook-instance*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AcceleratorTypes sagemaker:DirectInternetAccess sagemaker:InstanceTypes sagemaker:MinimumInstanceMetadataServiceVersion sagemaker:RootAccess	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateNotebookInstanceLifecycleConfig	Grants permission to create a notebook instance lifecycle configuration that can be deployed using Amazon SageMaker	Write	notebook-instance-lifecycle-config*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOptimizationJob	Grants permission to create an optimization job	Write	optimization-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerApp	Grants permission to create an Amazon SageMaker Partner AI App	Write	partner-app*		sagemaker:AddTags
				aws:RequestTag/${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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePresignedDomainUrl	Grants permission to return a URL that you can use from your browser to connect to the Domain as a specified UserProfile when AuthMode is 'IAM'	Write	user-profile*		
CreatePresignedMlflowAppUrl	Grants permission to return a URL that you can use from your browser to connect to the MLflow app	Write	mlflow-app*		
CreatePresignedMlflowTrackingServerUrl	Grants permission to return a URL that you can use from your browser to connect to the MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:RemoteAccess sagemaker:SpaceSharingType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:StudioLifecycleConfigArns	
CreateStudioLifecycleConfig	Grants permission to create a Studio Lifecycle Configuration that can be deployed using Amazon SageMaker	Write	studio-lifecycle-config*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingJob	Grants permission to start a model training job. After training completes, Amazon SageMaker saves the resulting model artifacts and other optional output to an Amazon S3 location that you specify	Write	training-job*		iam:PassRole sagemaker:AddTags
			reserved-capacity		
			training-plan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FileSystemAccessMode sagemaker:FileSystemDirectoryPath sagemaker:FileSystemId sagemaker:FileSystemType sagemaker:InstanceTypes sagemaker:InterContainerTra	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:KeepAlivePeriod	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:EnableRemoteDebu sagemaker:DirectGatedModelAccess	
CreateTrainingPlan	Grants permission to create a training plan that allocates resources for scheduling workloads within a specified time range	Write	training-plan*		sagemaker:AddTags sagemaker:CreateReservedCapacity
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransformJob	Grants permission to start a transform job. After the results are obtained, Amazon SageMaker saves them to an Amazon S3 location that you specify	Write	transform-job*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ModelArn sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	
CreateTrial	Grants permission to create a trial	Write	experiment*		sagemaker:AddTags
			experiment-trial*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrialComponent	Grants permission to create a trial component	Write	experiment-trial-component*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Grants permission to create a UserProfile for a SageMaker Domain	Write	user-profile*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:StudioLi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fecycleConfigArns	
CreateWorkforce	Grants permission to create a workforce	Write	workforce*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkteam	Grants permission to create a workteam	Write	workteam*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAction	Grants permission to delete an action	Write	action*		
DeleteAlgorithm	Grants permission to delete an algorithm	Write	algorithm*		
DeleteApp	Grants permission to delete an App	Write	app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
DeleteAppImageConfig	Grants permission to delete an AppImageConfig	Write	app-image-config*		
DeleteArtifact	Grants permission to delete an artifact	Write	artifact*		
DeleteAssociation	Grants permission to delete the association from a lineage entity (artifact, context, action, experiment, experiment-trial-component) to another	Write	action*		
			artifact*		
			context*		
			experiment*		
			experiment-trial-component*		
DeleteCluster	Grants permission to delete a SageMaker HyperPod cluster	Write	cluster*		eks:DeleteAccessEntry

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClusterSchedulerConfig	Grants permission to delete a cluster scheduler config	Write	cluster-scheduler-config*		
DeleteCodeRepository	Grants permission to delete a CodeRepository	Write	code-repository*		
DeleteCompilationJob	Grants permission to delete a compilation job	Write	compilation-job*		
DeleteComputeQuota	Grants permission to delete a compute quota	Write	compute-quota*		
DeleteContext	Grants permission to delete a context	Write	context*		
DeleteDataQualityJobDefinition	Grants permission to delete the data quality job definition created using the CreateDataQualityJobDefinition API	Write	data-quality-job-definition*		
DeleteDeviceFleet	Grants permission to delete a device fleet	Write	device-fleet*		
DeleteDomain	Grants permission to delete a Domain	Write	domain*		
DeleteEdgeDeploymentPlan	Grants permission to delete an edge deployment plan	Write	edge-deployment-plan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEdgeDeploymentStage	Grants permission to delete an edge deployment stage	Write	edge-deployment-plan*		
DeleteEndpoint	Grants permission to delete an endpoint. Amazon SageMaker frees up all the resources that were deployed when the endpoint was created	Write	endpoint*		
DeleteEndpointConfig	Grants permission to delete the endpoint configuration created using the CreateEndpointConfig API. The DeleteEndpointConfig API deletes only the specified configuration. It does not delete any endpoints created using the configuration	Write	endpoint-config*		
DeleteExperiment	Grants permission to delete an experiment	Write	experiment*		
DeleteFeatureGroup	Grants permission to delete a feature group	Write	feature-group*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFlowDefinition	Grants permission to delete the specified flow definition	Write	flow-definition*		
DeleteHub	Grants permission to delete hubs	Write	hub*		
DeleteHubContent	Grants permission to delete hub content	Write	hub*		
			hub-content*		
DeleteHubContentReference	Grants permission to delete hub content reference	Write	hub*		
			hub-content*		
DeleteHumanLoop	Grants permission to delete a specified human loop	Write	human-loop*		
DeleteHumanTaskUi	Grants permission to delete the specified human task user interface (worker task template)	Write	human-task-ui*		
DeleteHyperParameterTuningJob	Grants permission to delete a hyper parameter tuning job	Write	hyper-parameter-tuning-job*		
DeleteImage	Grants permission to delete a SageMaker Image	Write	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteImageVersion	Grants permission to delete a SageMaker ImageVersion	Write	image-version*		
DeleteInferenceComponent	Grants permission to delete an inference component. Amazon SageMaker frees up the resources that were reserved when the inference component was created	Write	inference-component*		
DeleteInferenceExperiment	Grants permission to delete an inference experiment	Write	inference-experiment*		
DeleteLineageGroupPolicy	Grants permission to delete a lineage group policy	Write			
DeleteMlflowApp	Grants permission to delete an MLflow app	Write	mlflow-app*		
DeleteMlflowTrackingServer	Grants permission to delete an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelPackage	Grants permission to delete a ModelPackage	Write	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
DeleteModelPackageGroup	Grants permission to delete a ModelPackageGroup	Write	model-package-group*		
DeleteModelPackageGroupPolicy	Grants permission to delete a ModelPackageGroup policy	Write	model-package-group*		
DeleteModelQualityJobDefinition	Grants permission to delete the model quality job definition created using the CreateModelQualityJobDefinition API	Write	model-quality-job-definition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy [permission only]	Grants AWS Resource Access Manager permission to delete a resource policy on a SageMaker resource that supports cross-account sharing	Write			
DeleteSpace	Grants permission to delete a Space	Write	space*		
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
DeleteStudioLifecycleConfig	Grants permission to delete a Studio Lifecycle Configuration	Write	studio-lifecycle-config*		
DeleteTags	Grants permission to delete the specified set of tags from an Amazon SageMaker resource	Tagging	action		
			algorithm		
			app		
			app-image-config		
			artifact		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			automl-job		
			cluster		
			cluster-scheduler-config		
			code-repository		
			compilation-job		
			compute-quota		
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		
			flow-definition		
			hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			hub-content		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		
			mlflow-app		
			mlflow-tracking-server		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			notebook-instance		
			notebook-instance-lifecycle-config		
			optimization-job		
			partner-app		
			pipeline		
			processing-job		
			project		
			reserved-capacity		
			space		
			studio-lifecycle-config		
			training-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			training-plan		
			transform-job		
			user-profile		
			workteam		
				aws: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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClusterEvent	Grants permission to return information about an Event within a SageMaker HyperPod cluster	Read	cluster*		
DescribeClusterInference [permission only]	Grants permission to get information about the inference operator for a SageMaker HyperPod cluster	Read	cluster*		
DescribeClusterNode	Grants permission to return information about a SageMaker HyperPod cluster node	Read	cluster*		
DescribeClusterSchedulerConfig	Grants permission to get information about a cluster scheduler config	Read	cluster-scheduler-config*		
DescribeCodeRepository	Grants permission to describe a CodeRepository	Read	code-repository*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeContext	Grants permission to get information about a context	Read	context*		
DescribeDataQualityJobDefinition	Grants permission to return information about a data quality job definition	Read	data-quality-job-definition*		
DescribeDevice	Grants permission to access information about a device	Read	device*		
DescribeDeviceFleet	Grants permission to access information about a device fleet	Read	device-fleet*		
DescribeDomain	Grants permission to describe a Domain	Read	domain*		
DescribeEdgeDeploymentPlan	Grants permission to access information about an edge deployment plan	Read	edge-deployment-plan*		
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			
DescribeMlflowApp	Grants permission to get information about an MLflow app	Read	mlflow-app*		
DescribeMlflowTrackingServer	Grants permission to get information about an MLflow tracking server	Read	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeModel	Grants permission to describe a model that you created using the CreateModel API	Read	model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelBiasJobDefinition	Grants permission to return information about a model bias job definition	Read	model-bias-job-definition*		
DescribeModelCard	Grants permission to get information about a model card	Read	model-card*		
DescribeModelCardExportJob	Grants permission to get information about a model card export job	Read	model-card-export-job*		
DescribeModelExplainabilityJobDefinition	Grants permission to return information about a model explainability job definition	Read	model-explainability-job-definition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelPackage	Grants permission to describe a ModelPackage	Read	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
DescribeModelPackageGroup	Grants permission to describe a ModelPackageGroup	Read	model-package-group*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNotebookInstance	Grants permission to return information about a notebook instance	Read	notebook-instance*		
DescribeNotebookInstanceLifecycleConfig	Grants permission to describe a notebook instance lifecycle configuration that was created via the CreateNotebookInstanceLifecycleConfig API	Read	notebook-instance-lifecycle-config*		
DescribeOptimizationJob	Grants permission to return information about an optimization job	Read	optimization-job*		
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*		
				sagemaker:PipelineVersionId	
DescribePipelineDefinitionForExecution	Grants permission to get the pipeline definition for a pipeline execution	Read	pipeline-execution*		
DescribePipelineExecution	Grants permission to get information about a pipeline execution	Read	pipeline-execution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProcessingJob	Grants permission to return information about a processing job	Read	processing-job*		
DescribeProject	Grants permission to describe a project	Read	project*		
DescribeReservedCapacity	Grants permission to return information about a specified Reserved Capacity	Read	reserved-capacity*		
DescribeSharedModel [permission only]	Grants permission to describe a shared model in a SageMaker Studio application	Read	shared-model*		
DescribeSpace	Grants permission to describe a Space	Read	space*		
DescribeStudioLifecycleConfig	Grants permission to describe a Studio Lifecycle Configuration	Read	studio-lifecycle-config*		
DescribeSubscribedWorkteam	Grants permission to return information about a subscribed workteam	Read	workteam*		
DescribeTrainingJob	Grants permission to return information about a training job	Read	training-job*		
DescribeTrainingPlan	Grants permission to return information about a specified training plan	Read	training-plan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribeUserProfile	Grants permission to describe a UserProfile	Read	user-profile*		
DescribeWorkforce	Grants permission to return information about a workforce	Read	workforce*		
DescribeWorkteam	Grants permission to return information about a workteam	Read	workteam*		
DetachClusterNodeVolume	Grants permission to detach an Amazon EBS volume from a SageMaker HyperPod cluster node	Write	cluster*		ec2:DescribeVolumes ec2:DetachVolume eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Resource Access Manager permission to retrieve a resource policy on a SageMaker resource that supports cross-account sharing	Read			
GetSagemakerServicecatalogPortfolioStatus	Grants permission to get a SageMaker Service Catalog Portfolio	Read			
GetScalingConfigurationRecommendation	Grants permission to get a scaling policy configuration recommendation	Read	inference-recommendations-job*		
GetSearchSuggestions	Grants permission to get search suggestions when provided with a keyword	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
InvokeEndpointAsync	Grants permission to get inferences from the hosted model at the specified endpoint in an asynchronous manner	Read	endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListAssociations	Grants permission to list associations	List			
ListAutoMLJobs	Grants permission to list AutoML jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCandidatesForAutoMLJob	Grants permission to lists candidates for an AutoML job	List			
ListClusterEvents	Grants permission to list events within a SageMaker HyperPod cluster	List	cluster*		
ListClusterNodes	Grants permission to list nodes within a SageMaker HyperPod cluster	List	cluster*		
ListClusterSchedulerConfigs	Grants permission to list cluster scheduler configs	List			
ListClusters	Grants permission to list SageMaker HyperPod clusters	List			
ListCodeRepositories	Grants permission to list code repositories	List			
ListCompilationJobs	Grants permission to list compilation jobs	List			
ListComputeQuotas	Grants permission to list compute quotas	List			
ListContexts	Grants permission to list contexts	List			
ListDataQualityJobDefinitions	Grants permission to list data quality job definitions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListFlowDefinitions	Grants permission to return summary information about flow definitions, given the specified parameters	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ListImages	Grants permission to list SageMaker Images in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListMlflowApps	Grants permission to list SageMaker MLflow Apps in your account	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			
ListNotebookInstances	Grants permission to list the Amazon SageMaker notebook instances in the requester's account in an AWS Region	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ListPipelineVersions	Grants permission to list versions of a pipeline	List	pipeline*		
ListPipelines	Grants permission to list pipelines	List			
ListProcessingJobs	Grants permission to list processing jobs	List			
ListProjects	Grants permission to list Projects	List			
ListResourceCatalogs	Grants permission to list resource catalogs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSharedModelEvents [permission only]	Grants permission to list shared model events	List			
ListSharedModelVersions [permission only]	Grants permission to list shared model versions	List	shared-model*		
ListSharedModels [permission only]	Grants permission to list shared models	List			
ListSpaces	Grants permission to list the Spaces in your account	List			
ListStageDevices	Grants permission to list stage devices	List			
ListStudioLifecycleConfigs	Grants permission to list the Studio Lifecycle Configurations that can be deployed using Amazon SageMaker	List			
ListSubscribedWorkteams	Grants permission to list subscribed workteams	List			
ListTags	Grants permission to list the tag set associated with the specified resource	List	action		
			algorithm		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			cluster-scheduler-config		
			code-repository		
			compilation-job		
			compute-quota		
			context		
			data-quality-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			flow-definition		
			hub		
			hub-content		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mlflow-app		
			mlflow-tracking-server		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			notebook-instance		
			notebook-instance-lifecycle-config		
			optimization-job		
			partner-app		
			pipeline		
			pipeline-execution		
			processing-job		
			project		
			reserved-capacity		
			space		
			studio-lifecycle-config		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			training-job		
			training-plan		
			transform-job		
			user-profile		
			workteam		
ListTrainingJobs	Grants permission to list training jobs	List			
ListTrainingJobsForHyperParameterTuningJob	Grants permission to list training jobs for a hyper parameter tuning job	List	hyper-parameter-tuning-job*		
ListTrainingPlans	Grants permission to list all the training plans that have been created in a specified account	List			
ListTransformJobs	Grants permission to list transform jobs	List			
ListTrialComponents	Grants permission to list trial components	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrials	Grants permission to list trials	List			
ListUltraServersByReservedCapacity	Grants permission to list all UltraServers in a specified Reserved Capacity	List	reserved-capacity*		
ListUserProfiles	Grants permission to list the UserProfiles in your account	List			
ListWorkforces	Grants permission to list workforces	List			
ListWorkteams	Grants permission to list workteams	List			
PutLineageGroupPolicy	Grants permission to put a lineage group policy	Write			
PutModelPackageGroupPolicy	Grants permission to put a ModelPackageGroup policy	Write	model-package-group*		
PutRecord	Grants permission to put a record to a feature group	Write	feature-group*		
PutResourcePolicy [permission only]	Grants AWS Resource Access Manager permission to create a resource policy on a SageMaker resource that supports cross-account sharing	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
QueryLineage	Grants permission to explore the lineage graph	List			
RegisterDevices	Grants permission to register a set of devices	Write	device*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenderUiTemplate	Grants permission to render a UI template used for a human annotation task	Read			iam:PassRole
RetryPipelineExecution	Grants permission to retry a pipeline execution	Write	pipeline-execution*		
Search	Grants permission to search for SageMaker objects	Read		sagemaker:SearchVisibilityCondition/${FilterKey}	
SearchTrainingPlanOfferings	Grants permissions to search for the available training plan offerings that best match specified capacity requirements	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendHeartbeat	Grants permission to publish heartbeat data from devices. After you deploy a model onto edge devices this api is used to report device status	Write	device*		
SendPipelineExecutionStepFailure	Grants permission to fail a pending callback step	Write	pipeline-execution*		
SendPipelineExecutionStepSuccess	Grants permission to succeed a pending callback step	Write	pipeline-execution*		
SendSharedModelEvent [permission only]	Grants permission to send a shared model event	Write	shared-model-event*		
StartEdgeDeploymentStage	Grants permission to start an edge deployment stage	Write	edge-deployment-plan*		
StartHumanLoop	Grants permission to start a human loop	Write	flow-definition*		
StartInferenceExperiment	Grants permission to start an inference experiment	Write	inference-experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMlflowTrackingServer	Grants permission to start an MLfLow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartMonitoringSchedule	Grants permission to start a monitoring schedule	Write	monitoring-schedule*		
StartNotebookInstance	Grants permission to start a notebook instance. This launches an EC2 instance with the latest version of the libraries and attaches your EBS volume	Write	notebook-instance*		
StartPipelineExecution	Grants permission to start a pipeline execution	Write	pipeline*		
				sagemaker:PipelineVersionId	
StartSession	Grants permission to start a remote session for a SageMaker space	Write	space*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopAutoMLJob	Grants permission to stop a running AutoML job	Write	automl-job*		
StopCompilationJob	Grants permission to stop a compilation job	Write	compilation-job*		
StopEdgeDeploymentStage	Grants permission to stop an edge deployment stage	Write	edge-deployment-plan*		
StopEdgePackagingJob	Grants permission to stop an edge packaging job	Write	edge-packaging-job*		
StopHumanLoop	Grants permission to stop a specified human loop	Write	human-loop*		
StopHyperParameterTuningJob	Grants permission to stop a running hyper parameter tuning job create via the CreateHyperParameterTuningJob	Write	hyper-parameter-tuning-job*		
StopInferenceExperiment	Grants permission to stop an inference experiment	Write	inference-experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopInferenceRecommendationsJob	Grants permission to stop an inference recommendations job	Write	inference-recommendations-job*		
StopLabelingJob	Grants permission to stop a labeling job. Any labels already generated will be exported before stopping	Write	labeling-job*		
StopMlflowTrackingServer	Grants permission to stop an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StopMonitoringSchedule	Grants permission to stop a monitoring schedule	Write	monitoring-schedule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopNotebookInstance	Grants permission to stop a notebook instance. This terminates the EC2 instance. Before terminating the instance, Amazon SageMaker disconnects the EBS volume from it. Amazon SageMaker preserves the EBS volume	Write	notebook-instance*		
StopOptimizationJob	Grants permission to stop an optimization job	Write	optimization-job*		
StopPipelineExecution	Grants permission to stop a pipeline execution	Write	pipeline-execution*		
StopProcessingJob	Grants permission to stop a processing job. To stop a job, Amazon SageMaker sends the algorithm the SIGTERM signal, which delays job termination for 120 seconds	Write	processing-job*		
StopTrainingJob	Grants permission to stop a training job. To stop a job, Amazon SageMaker sends the algorithm the SIGTERM signal, which delays job termination for 120 seconds	Write	training-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopTransformJob	Grants permission to stop a transform job. When Amazon SageMaker receives a StopTransformJob request, the status of the job changes to Stopping. After Amazon SageMaker stops the job, the status is set to Stopped	Write	transform-job*		
TrainHubModel	Grants permission to train a model in hub	Write	hub*		
			hub-content*		
UpdateAction	Grants permission to update an action	Write	action*		
UpdateAppImageConfig	Grants permission to update an AppImageConfig	Write	app-image-config*		
UpdateArtifact	Grants permission to update an artifact	Write	artifact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	Grants permission to update a SageMaker HyperPod cluster	Write	cluster*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyImageAttribute ec2:ModifySnapshotAttribute eks:AssociateAccessPolicy eks:CreateAccessEntry eks:DeleteAccessEntry eks:DescribeAccessEntry eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PassRole sagemaker:BatchAddClusterNodes sagemaker:BatchDeleteClusterNodes
			reserved-capacity		
			training-plan		
				sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateClusterInference [permission only]	Grants permission to update the inference operator for a SageMaker HyperPod cluster	Write	cluster*		eks:AssociateAccessPolicy eks:DescribeCluster eks:ListAssociatedAccessPolicies iam:PassRole sagemaker:DescribeCluster
UpdateClusterSchedulerConfig	Grants permission to update a cluster scheduler config	Write	cluster-scheduler-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateClusterSoftware	Grants permission to update platform software for a SageMaker HyperPod cluster	Write	cluster*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyImageAttribute ec2:ModifySnapshotAttribute eks:DescribeCluster
UpdateCodeRepository	Grants permission to update a CodeRepository	Write	code-repository*		
UpdateComputeQuota	Grants permission to update a compute quota	Write	compute-quota*		
UpdateContext	Grants permission to update a context	Write	context*		
UpdateDeviceFleet	Grants permission to update a device fleet	Write	device-fleet*		
UpdateDevices	Grants permission to update a set of devices	Write	device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDomain	Grants permission to update a Domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:AppNetworkAccessType sagemaker:VpcSubnets sagemaker:StudioLi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fecycleConfigArns	
UpdateEndpoint	Grants permission to update an endpoint to use the endpoint configuration specified in the request	Write	endpoint*		
			endpoint-config*		
UpdateEndpointWeightsAndCapacities	Grants permission to update variant weight, capacity, or both of one or more variants associated with an endpoint	Write	endpoint*		
UpdateExperiment	Grants permission to update an experiment	Write	experiment*		
UpdateFeatureGroup	Grants permission to update a feature group	Write	feature-group*		
UpdateFeatureMetadata	Grants permission to update a feature metadata	Write	feature-group*		
UpdateHub	Grants permission to update hubs	Write	hub*		
UpdateHubContent	Grants permission to update hub content	Write	hub*		
			hub-content*		
UpdateHubContentReference	Grants permission to update hub content reference	Write	hub*		
			hub-content*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateImage	Grants permission to update the properties of a SageMaker Image	Write	image*		iam:PassRole
UpdateImageVersion	Grants permission to update the properties of a SageMaker ImageVersion	Write	image-version*		
UpdateInferenceComponent	Grants permission to update an inference component to use the specification and configurations specified in the request	Write	inference-component*		
UpdateInferenceComponentRuntimeConfig	Grants permission to update the runtime config of a given inference component	Write	inference-component*		
UpdateInferenceExperiment	Grants permission to update an inference experiment	Write	inference-experiment*		
UpdateMlflowApp	Grants permission to update an MLflow app	Write	mlflow-app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMlflowTrackingServer	Grants permission to update an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateModelCard	Grants permission to update a model card	Write	model-card*		
UpdateModelPackage	Grants permission to update a ModelPackage	Write	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:ModelApprovalStatus sagemaker:CustomerMetadataProperties/${MetadataKey} sagemaker:CustomerMetadataPropertiesToRemove sagemaker:ModelLifeCycle:Stage sagemaker:ModelLifeCycle:StageStatus	
UpdateMonitoringAlert	Grants permission to update a monitoring alert	Write	monitoring-schedule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			monitoring-schedule-alert*		
UpdateMonitoringSchedule	Grants permission to update a monitoring schedule	Write	monitoring-schedule*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSubnets sagemaker:InterContainerTrafficEncryption	
UpdateNotebookInstance	Grants permission to update a notebook instance. Notebook instance updates include upgrading or downgrading the EC2 instance used for your notebook instance to accommodate changes in your workload requirements	Write	notebook-instance*	sagemaker:AcceleratorTypes sagemaker:InstanceTypes sagemaker:MinimumInstanceMetadataServiceVersion sagemaker:RootAccess	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotebookInstanceLifecycleConfig	Grants permission to updates a notebook instance lifecycle configuration created with the CreateNotebookInstanceLifecycleConfig API	Write	notebook-instance-lifecycle-config*		
UpdatePartnerApp	Grants permission to update an Amazon SageMaker Partner AI App	Write	partner-app*		
UpdatePipeline	Grants permission to update a pipeline	Write	pipeline*		iam:PassRole
UpdatePipelineExecution	Grants permission to update a pipeline execution	Write	pipeline-execution*		
UpdatePipelineVersion	Grants permission to update a pipeline version	Write	pipeline*		
				sagemaker:PipelineVersionId	
UpdateProject	Grants permission to update a Project	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSharedModel [permission only]	Grants permission to update a shared model	Write	shared-model*		
UpdateSpace	Grants permission to update a Space	Write	space*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:RemoteAccess sagemaker:SpaceSharingType sagemaker:StudioLifecycleConfigArns	
UpdateTrainingJob	Grants permission to update a training job	Write	training-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:KeepAlivePeriod sagemaker:EnableRemoteDebu	
UpdateTrial	Grants permission to update a trial	Write	experiment-trial*		
UpdateTrialComponent	Grants permission to update a trial component	Write	experiment-trial-component*		
UpdateUserProfile	Grants permission to update a UserProfile	Write	user-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:StudioLifecycleConfigArns	
UpdateWorkforce	Grants permission to update a workforce	Write	workforce*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWorkteam	Grants permission to update a workteam	Write	workteam*		

Resource types defined by Amazon SageMaker

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
device	`arn:${Partition}:sagemaker:${Region}:${Account}:device-fleet/${DeviceFleetName}/device/${DeviceName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
device-fleet	`arn:${Partition}:sagemaker:${Region}:${Account}:device-fleet/${DeviceFleetName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
edge-packaging-job	`arn:${Partition}:sagemaker:${Region}:${Account}:edge-packaging-job/${EdgePackagingJobName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
edge-deployment-plan	arn:${Partition}:sagemaker:${Region}:${Account}:edge-deployment/${EdgeDeploymentPlanName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-loop	arn:${Partition}:sagemaker:${Region}:${Account}:human-loop/${HumanLoopName}	
flow-definition	arn:${Partition}:sagemaker:${Region}:${Account}:flow-definition/${FlowDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-task-ui	arn:${Partition}:sagemaker:${Region}:${Account}:human-task-ui/${HumanTaskUiName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hub	arn:${Partition}:sagemaker:${Region}:${Account}:hub/${HubName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hub-content	arn:${Partition}:sagemaker:${Region}:${Account}:hub-content/${HubName}/${HubContentType}/${HubContentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
inference-recommendations-job	arn:${Partition}:sagemaker:${Region}:${Account}:inference-recommendations-job/${InferenceRecommendationsJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
inference-experiment	arn:${Partition}:sagemaker:${Region}:${Account}:inference-experiment/${InferenceExperimentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
labeling-job	arn:${Partition}:sagemaker:${Region}:${Account}:labeling-job/${LabelingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
workteam	arn:${Partition}:sagemaker:${Region}:${Account}:workteam/${WorkteamName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
workforce	arn:${Partition}:sagemaker:${Region}:${Account}:workforce/${WorkforceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
domain	arn:${Partition}:sagemaker:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
user-profile	arn:${Partition}:sagemaker:${Region}:${Account}:user-profile/${DomainId}/${UserProfileName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
space	arn:${Partition}:sagemaker:${Region}:${Account}:space/${DomainId}/${SpaceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
app	arn:${Partition}:sagemaker:${Region}:${Account}:app/${DomainId}/${UserProfileName}/${AppType}/${AppName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
app-image-config	arn:${Partition}:sagemaker:${Region}:${Account}:app-image-config/${AppImageConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
studio-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:studio-lifecycle-config/${StudioLifecycleConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
notebook-instance	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance/${NotebookInstanceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
notebook-instance-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance-lifecycle-config/${NotebookInstanceLifecycleConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
code-repository	arn:${Partition}:sagemaker:${Region}:${Account}:code-repository/${CodeRepositoryName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
image	arn:${Partition}:sagemaker:${Region}:${Account}:image/${ImageName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
image-version	arn:${Partition}:sagemaker:${Region}:${Account}:image-version/${ImageName}/${Version}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
algorithm	arn:${Partition}:sagemaker:${Region}:${Account}:algorithm/${AlgorithmName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
cluster	arn:${Partition}:sagemaker:${Region}:${Account}:cluster/${ClusterId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
training-job	arn:${Partition}:sagemaker:${Region}:${Account}:training-job/${TrainingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
processing-job	arn:${Partition}:sagemaker:${Region}:${Account}:processing-job/${ProcessingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hyper-parameter-tuning-job	arn:${Partition}:sagemaker:${Region}:${Account}:hyper-parameter-tuning-job/${HyperParameterTuningJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
training-plan	arn:${Partition}:sagemaker:${Region}:${Account}:training-plan/${TrainingPlanName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
reserved-capacity	arn:${Partition}:sagemaker:${Region}:${Account}:reserved-capacity/${RandomString}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
project	arn:${Partition}:sagemaker:${Region}:${Account}:project/${ProjectName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
model-package	arn:${Partition}:sagemaker:${Region}:${Account}:model-package/${ModelPackageName}	aws:ResourceTag/${TagKey} sagemaker:CurrentCustomerMetadataProperties/${MetadataKey} sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentModelLifeCycleStageStatus sagemaker:ResourceTag/${TagKey}
model-package-group	arn:${Partition}:sagemaker:${Region}:${Account}:model-package-group/${ModelPackageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model	arn:${Partition}:sagemaker:${Region}:${Account}:model/${ModelName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
endpoint-config	arn:${Partition}:sagemaker:${Region}:${Account}:endpoint-config/${EndpointConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
endpoint	arn:${Partition}:sagemaker:${Region}:${Account}:endpoint/${EndpointName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
inference-component	arn:${Partition}:sagemaker:${Region}:${Account}:inference-component/${InferenceComponentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
transform-job	arn:${Partition}:sagemaker:${Region}:${Account}:transform-job/${TransformJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
compilation-job	arn:${Partition}:sagemaker:${Region}:${Account}:compilation-job/${CompilationJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
optimization-job	arn:${Partition}:sagemaker:${Region}:${Account}:optimization-job/${OptimizationJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
automl-job	arn:${Partition}:sagemaker:${Region}:${Account}:automl-job/${AutoMLJobJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
monitoring-schedule	arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
monitoring-schedule-alert	arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}/alert/${MonitoringScheduleAlertName}	
data-quality-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:data-quality-job-definition/${DataQualityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-quality-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-quality-job-definition/${ModelQualityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-bias-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-bias-job-definition/${ModelBiasJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-explainability-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-explainability-job-definition/${ModelExplainabilityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
experiment	arn:${Partition}:sagemaker:${Region}:${Account}:experiment/${ExperimentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
experiment-trial	arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial/${TrialName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
experiment-trial-component	arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial-component/${TrialComponentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
feature-group	arn:${Partition}:sagemaker:${Region}:${Account}:feature-group/${FeatureGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline-execution	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}/execution/${RandomString}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
artifact	arn:${Partition}:sagemaker:${Region}:${Account}:artifact/${HashOfArtifactSource}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
context	arn:${Partition}:sagemaker:${Region}:${Account}:context/${ContextName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
action	arn:${Partition}:sagemaker:${Region}:${Account}:action/${ActionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
lineage-group	arn:${Partition}:sagemaker:${Region}:${Account}:lineage-group/${LineageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-card	arn:${Partition}:sagemaker:${Region}:${Account}:model-card/${ModelCardName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-card-export-job	arn:${Partition}:sagemaker:${Region}:${Account}:model-card/${ModelCardName}/export-job/${ExportJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
shared-model	arn:${Partition}:sagemaker:${Region}:${Account}:shared-model/${SharedModelId}	
shared-model-event	arn:${Partition}:sagemaker:${Region}:${Account}:shared-model-event/${EventId}	
sagemaker-catalog	arn:${Partition}:sagemaker:${Region}:${Account}:sagemaker-catalog/${ResourceCatalogName}	
mlflow-tracking-server	arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}	
mlflow-app	arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-app/${MLflowAppId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
compute-quota	arn:${Partition}:sagemaker:${Region}:${Account}:compute-quota/${ComputeQuotaId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
cluster-scheduler-config	arn:${Partition}:sagemaker:${Region}:${Account}:cluster-scheduler-config/${ClusterSchedulerConfigId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the SageMaker service	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String
aws:TagKeys	Filters access by the list of all the tag key names associated with the resource in the request	ArrayOfString
sagemaker:AcceleratorTypes	Filters access by the list of all accelerator types associated with the resource in the request	ArrayOfString
sagemaker:AppNetworkAccessType	Filters access by the app network access type associated with the resource in the request	String

Condition keys	Description	Type
sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	Filters access by a current metadata key and value pair associated with the model-package resource	String
sagemaker:CurrentModelLifeCycleStage	Filters access by the current value of the Stage field in the model life cycle object associated with the model-package resource	String
sagemaker:CurrentModelLifeCycleStageStatus	Filters access by the current value of the StageStatus field in the model life cycle object associated with the model-package resource	String
sagemaker:CustomerMetadataProperties/${MetadataKey}	Filters access by a metadata key and value pair	String
sagemaker:CustomerMetadataPropertiesToRemove	Filters access by the list of metadata properties associated with the model-package resource in the request	ArrayOfString
sagemaker:DirectGatedModelAccess	Used to deny direct access to SageMaker gated ModelReferences	String
sagemaker:DirectInternetAccess	Filters access by the direct internet access associated with the resource in the request	String

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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
sagemaker:PipelineVersionId	Filters access to specific version IDs of a Sagemaker pipeline	String
sagemaker:RemoteAccess	Filters access by the remote access flag associated with the space in the request	String
sagemaker:ResourceTag/	Filters access by the preface string for a tag key and value pair attached to a resource	String
sagemaker:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String
sagemaker:RootAccess	Filters access by the root access associated with the resource in the request	String
sagemaker:SearchVisibilityCondition/${FilterKey}	Limits the results of your search request to the resources that you can access. ${FilterKey} is a key that the VisibilityConditions configuration presents in the Search request	String

Condition keys	Description	Type
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:StudioLifecycleConfigArns	Filters access by the list of lifecycle configuration ARNs associated with the resource in the request	ArrayOfARN
sagemaker:TaggingAction	Filters access by the API actions to which a user can apply tags. Uses the name of the API operation that creates a taggable resource to filter access	String
sagemaker:TargetModel	Filters access by the target model associated with the Multi-Model Endpoint in the request	String
sagemaker:UserProfileName	You can use the UserProfileName as a policy variable to filter requests from specific user profiles within a SageMaker Domain. This context key is not applicable to user profiles within shared spaces	String
sagemaker:VolumeKmsKey	Filters access by the volume kms key associated with the resource in the request	ARN
sagemaker:VpcSecurityGroupIds	Filters access by the list of all VPC security group ids associated with the resource in the request	ArrayOfString

Condition keys	Description	Type
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 SageMaker data science assistant

Amazon SageMaker data science assistant (service prefix: `sagemaker-data-science-assistant`) 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 data science assistant
- Resource types defined by Amazon SageMaker data science assistant
- Condition keys for Amazon SageMaker data science assistant

Actions defined by Amazon SageMaker data science assistant

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendConversation [permission only]	Grants permission to start a conversation with SageMaker data science assistant	Write			

Resource types defined by Amazon SageMaker data science assistant

Amazon SageMaker data science assistant does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon SageMaker data science assistant, specify `"Resource": "*"` in your policy.

Condition keys for Amazon SageMaker data science assistant

SageMakerDataScienceAssistant has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon SageMaker geospatial capabilities

Amazon SageMaker geospatial capabilities (service prefix: `sagemaker-geospatial`) 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 geospatial capabilities

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEarthObservationJob	Grants permission to the DeleteEarthObservationJob operation which deletes an existing earth observation job	Write	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
DeleteVectorEnrichmentJob	Grants permission to the DeleteVectorEnrichmentJob operation which deletes an existing vector enrichment job	Write	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ExportEarthObservationJob	Grants permission to copy results of an earth observation job to an S3 location	Write	EarthObservationJob*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ExportVectorEnrichmentJob	Grants permission to copy results of an VectorEnrichmentJob to an S3 location	Write	VectorEnrichmentJob*		iam:PassRole
				aws:ResourceTag/${TagKey}	
GetEarthObservationJob	Grants permission to return details about the earth observation job	Read	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
GetRasterDataCollection	Grants permission to return details about the raster data collection	Read	RasterDataCollection*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTile	Grants permission to get the tile of an earth observation job	Read	EarthObservationJob*		iam:PassRole
GetVectorEnrichmentJob	Grants permission to return details about the vector enrichment job	Read	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	
ListEarthObservationJobs	Grants permission to return an array of earth observation jobs associated with the current account	List			
ListRasterDataCollections	Grants permission to return an array of aster data collections associated with the given model name	List			
ListTagsForResource	Grants permission to lists tag for an SageMaker Geospatial resource	List	EarthObservationJob		
			RasterDataCollection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VectorEnrichmentJob		
				aws:ResourceTag/${TagKey}	
ListVectorEnrichmentJobs	Grants permission to return an array of vector enrichment jobs associated with the current account	List			
SearchRasterDataCollection	Grants permission to query raster data collections	Read			
StartEarthObservationJob	Grants permission to the StartEarthObservationJob operation which starts a new earth observation job to your account	Write	EarthObservationJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartVectorEnrichmentJob	Grants permission to the StartVectorEnrichmentJob operation which starts a new vector enrichment job to your account	Write	VectorEnrichmentJob*		iam:PassRole sagemaker-geospatial:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StopEarthObservationJob	Grants permission to the StopEarthObservationJob operation which stops an existing earth observation job	Write	EarthObservationJob*		
				aws:ResourceTag/${TagKey}	
StopVectorEnrichmentJob	Grants permission to the StopVectorEnrichmentJob operation which stops an existing vector enrichment job	Write	VectorEnrichmentJob*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an SageMaker Geospatial resource	Tagging	EarthObservationJob		
			RasterDataCollection		
			VectorEnrichmentJob		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an SageMaker Geospatial resource	Tagging	EarthObservationJob		
			RasterDataCollection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VectorEnrichmentJob		
				aws:TagKeys	

Resource types defined by Amazon SageMaker geospatial capabilities

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
EarthObservationJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:earth-observation-job/${JobID}`	aws:ResourceTag/${TagKey}
RasterDataCollection	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:raster-data-collection/${CollectionID}`	aws:ResourceTag/${TagKey}
VectorEnrichmentJob	`arn:${Partition}:sagemaker-geospatial:${Region}:${Account}:vector-enrichment-job/${JobID}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon SageMaker geospatial capabilities

Amazon SageMaker geospatial capabilities defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon SageMaker Unified Studio MCP

Amazon SageMaker Unified Studio MCP (service prefix: `sagemaker-unified-studio-mcp`) 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 Unified Studio MCP

- Resource types defined by Amazon SageMaker Unified Studio MCP
- Condition keys for Amazon SageMaker Unified Studio MCP

Actions defined by Amazon SageMaker Unified Studio MCP

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CallPrivilegedTool [permission only]	Grants permission to call privileged tools in MCP service	Write			
CallReadOnlyTool [permission only]	Grants permission to call read-only tools in MCP service	Read			
InvokeMcp [permission only]	Grants permission to use MCP service	Read			

Resource types defined by Amazon SageMaker Unified Studio MCP

Amazon SageMaker Unified Studio MCP does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon SageMaker Unified Studio MCP, specify `"Resource": "*"` in your policy.

Condition keys for Amazon SageMaker Unified Studio MCP

SageMaker Unified Studio MCP has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon SageMaker with MLflow

Amazon SageMaker with MLflow (service prefix: `sagemaker-mlflow`) 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 with MLflow
- Resource types defined by Amazon SageMaker with MLflow
- Condition keys for Amazon SageMaker with MLflow

Actions defined by Amazon SageMaker with MLflow

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessUI	Grants permission to access the MLflow UI	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExperiment	Grants permission to create an MLflow experiment	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
CreateModelVersion	Grants permission to create a new model version	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
CreateRegisteredModel	Grants permission to create a registered model	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
CreateRun	Grants permission to create a new run within an experiment	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteExperiment	Grants permission to mark an MLflow experiment for deletion	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteLoggedModel	Grants permission to delete a logged model in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLoggedModelTag	Grants permission to delete a tag for a logged model in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteModelVersion	Grants permission to delete a model version	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteModelVersionTag	Grants permission to delete a model version tag	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRegisteredModel	Grants permission to delete a registered model	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRegisteredModelAlias	Grants permission to delete a registered model alias	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteRegisteredModelTag	Grants permission to delete a registered model tag	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRun	Grants permission to mark a run for deletion	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteTag	Grants permission to delete a tag on a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteTraceTag	Grants permission to delete a trace tag in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
DeleteTraces	Grants permission to delete traces in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
EndTrace	Grants permission to end a trace in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
FinalizeLoggedModel	Grants permission to set status for a logged model in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDownloadURIForModelVersionArtifacts	Grants permission to get a URI to download model artifacts for a specific model version	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetExperiment	Grants permission to get metadata for an MLflow experiment	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetExperimentByName	Grants permission to get metadata for an MLflow experiment by name	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetLatestModelVersions	Grants permission to get the latest model versions	List	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetLoggedModel	Grants permission to get a logged model in MLflow	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetMetricHistory	Grants permission to get a list of all values for the specified metric for a given run	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetModelVersion	Grants permission to get a model version by model name and version	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetModelVersionByAlias	Grants permission to get model version by alias in MLflow	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetRegisteredModel	Grants permission to get a registered model	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetRun	Grants permission to get metadata, metrics, parameters, and tags for a run	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
GetTraceInfo	Grants permission to get information about a trace in MLflow	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
ListArtifacts	Grants permission to list artifacts for a run	List	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLoggedModelArtifacts	Grants permission to list artifacts for a logged model in MLflow	List	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogBatch	Grants permission to log a batch of metrics, parameters, and tags for a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogInputs	Grants permission to log inputs for a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogLoggedModelParams	Grants permission to log params for a logged model in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogMetric	Grants permission to log a metric for a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogModel	Grants permission to log the model associated with a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LogOutputs	Grants permission to log outputs, such as models, for a run in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
LogParam	Grants permission to log a parameter tracked during a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
RenameRegisteredModel	Grants permission to rename a registered model	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
RestoreExperiment	Grants permission to restore an experiment marked for deletion	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
RestoreRun	Grants permission to restore a deleted run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchExperiments	Grants permission to search for MLflow experiments	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchLoggedModels	Grants permission to search for logged models in MLflow	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchModelVersions	Grants permission to search for a model version	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchRegisteredModels	Grants permission to search for registered models in MLflow	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchRuns	Grants permission to search for runs that satisfy expressions	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SearchTraces	Grants permission to search for traces in MLflow	Read	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetExperimentTag	Grants permission to set a tag on an experiment	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLoggedModelTags	Grants permission to set tags for a logged model in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetModelVersionTag	Grants permission to set a tag for the model version	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetRegisteredModelAlias	Grants permission to set a registered model alias	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetRegisteredModelTag	Grants permission to set a tag for a registered model	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetTag	Grants permission to set a tag on a run	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
SetTraceTag	Grants permission to set a trace tag in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTrace	Grants permission to start a trace in MLflow	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
TransitionModelVersionStage	Grants permission to transition a model version to a particular stage	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateExperiment	Grants permission to update the metadata for an MLflow experiment	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateModelVersion	Grants permission to update the model version	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateRegisteredModel	Grants permission to update a registered model	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	
UpdateRun	Grants permission to update run metadata	Write	mlflow-tracking-server*	aws:ResourceTag/${TagKey}	

Resource types defined by Amazon SageMaker with MLflow

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
mlflow-tracking-server	`arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}`	

Condition keys for Amazon SageMaker with MLflow

Amazon SageMaker with MLflow defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String

Actions, resources, and condition keys for AWS Savings Plans

AWS Savings Plans (service prefix: `savingsplans`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Savings Plans

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSavingsPlan	Grants permission to create a savings plan	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Grants permission to delete the queued savings plan associated with customers account	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSavingsPlanRates	Grants permission to describe the rates associated with customers savings plan	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	Grants permission to describe the savings plans associated with customers account	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Grants permission to describe the rates 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a savings plan	Tagging	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a savings plan	Tagging	savingsplan*		
				aws:TagKeys	

Resource types defined by AWS Savings Plans

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Savings Plans

AWS Savings Plans defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Secrets Manager

AWS Secrets Manager (service prefix: `secretsmanager`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Secrets Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetSecretValue	Grants permission to retrieve and decrypt a list of secrets	List			
CancelRotateSecret	Grants permission to cancel an in-progress secret rotation	Write	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
CreateSecret	Grants permission to create a secret that stores encrypted data that can be queried and rotated	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:AddReplicaRegions secretsmanager:ForceOverwriteReplicaSecret secretsmanager:Type	
DeleteResourcePolicy	Grants permission to delete the resource policy attached to a secret	Permissions management	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
DeleteSecret	Grants permission to delete a secret	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
DescribeSecret	Grants permission to retrieve the metadata about a secret, but not the encrypted data	Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRandomPassword	Grants permission to generate a random string for use in password creation	Read			
GetResourcePolicy	Grants permission to get the resource policy attached to a secret	Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
GetSecretValue		Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve and decrypt the encrypted data				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:resource/Type	
ListSecretVersionIds	Grants permission to list the available versions of a secret	Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
ListSecrets	Grants permission to list the available secrets	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to attach a resource policy to a secret	Permissions management	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion secretsmanager:res	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ource/ Type	
PutSecret Value	Grants permission to create a new version of the secret with new encrypted data	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
	Grants permission to remove regions from replication	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveRegionsFromReplication				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 secretsmanager:resource/Type	
RestoreSecret	Grants permission to cancel deletion of a secret	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
RotateSecret	Grants permission to start rotation of a secret	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaAr n secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:Mod	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ifyRotationRules secretsmanager:RotateImmediately secretsmanager:resource/Type secretsmanager:ExternalSecretRotationRoleArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopReplicationToReplica	Grants permission to remove the secret from replication and promote the secret to a regional secret in the replica Region	Write	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a secret	Tagging	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:resource/Type	
UntagResource	Grants permission to remove tags from a secret	Tagging	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecret	Grants permission to update a secret with new metadata or with a new version of the encrypted data	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretPrimaryRegion secretsmanager:Type secretsmanager:resource/Type	
UpdateSecretVersionStage	Grants permission to move a stage from one secret to another	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:res	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ource/ Type	
ValidateResourcePolicy	Grants permission to validate a resource policy before attaching policy	Permissions management	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Resource types defined by AWS Secrets Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn secretsmanager:resource/Type

Condition keys for AWS Secrets Manager

AWS Secrets Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the Secrets Manager service	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the list of all the tag key names present in the request the user makes to the Secrets Manager service	ArrayOfString
secretsmanager:AddReplicaRegions	Filters access by the list of Regions in which to replicate the secret	ArrayOfString
secretsmanager:BlockPublicPolicy	Filters access by whether the resource policy blocks broad AWS account access	Bool
secretsmanager:Description	Filters access by the description text in the request	String
secretsmanager:ExternalSecretRotationRoleArn	Filters access by the managed external secret rotation role ARN in the request	ARN
secretsmanager:ForceDeleteWithoutRecovery	Filters access by whether the secret is to be deleted immediately without any recovery window	Bool
secretsmanager:For	Filters access by whether to overwrite a secret with the same name in the destination Region	Bool

Condition keys	Description	Type
ceOverwriteReplicaSecret		
secretsmanager:KmsKeyArn	Filters access by the key ARN of the KMS key in the request	ARN
secretsmanager:KmsKeyId	Filters access by the key identifier of the KMS key in the request. Deprecated: Use secretsmanager:KmsKeyArn	String
secretsmanager:ModifyRotationRules	Filters access by whether the rotation rules of the secret are to be modified	Bool
secretsmanager:Name	Filters access by the friendly name of the secret in the request	String
secretsmanager:RecoveryWindowInDays	Filters access by the number of days that Secrets Manager waits before it can delete the secret	Numeric
secretsmanager:ResourceTag/tag-key	Filters access by a tag key and value pair	String
secretsmanager:RotateImmediately	Filters access by whether the secret is to be rotated immediately	Bool
secretsmanager:RotationLambdaARN	Filters access by the ARN of the rotation Lambda function in the request	ARN

Condition keys	Description	Type
secretsmanager:SecretId	Filters access by the SecretID value in the request	ARN
secretsmanager:SecretPrimaryRegion	Filters access by primary region in which the secret is created if the secret is a multi-Region secret	String
secretsmanager:Type	Filters access by the managed external secret type in the request	String
secretsmanager:VersionId	Filters access by the unique identifier of the version of the secret in the request	String
secretsmanager:VersionStage	Filters access by the list of version stages in the request	String
secretsmanager:resource/AllowRotationLambdaArn	Filters access by the ARN of the rotation Lambda function associated with the secret	ARN
secretsmanager:resource/Type	Filters access by the managed external secret type associated with the secret	String

Actions, resources, and condition keys for AWS Security Agent

AWS Security Agent (service prefix: `securityagent`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Security Agent

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddArtifact	Grants permission to add an Artifact for the given Agent Space	Write	AgentSpace*		
BatchDeletePentests	Grants permission to delete multiple penetration tests in a single request	Write	AgentSpace*		kms:Decrypt
BatchGetAgentSpaces	Grants permission to retrieve multiple agent spaces in a single request	Read	AgentSpace*		kms:Decrypt
BatchGetArtifactMetadata	Grants permission to retrieve one or more Artifact Metadata records for the given Agent Space	Read	AgentSpace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetFindings	Grants permission to retrieve multiple security testing findings in a single request	Read	AgentSpace*		kms:Decrypt
BatchGetPentestJobContentMetadata	Grants permission to retrieve multiple pentest job contents metadata in a single request	Read	AgentSpace*		kms:Decrypt
BatchGetPentestJobTasks	Grants permission to retrieve multiple pentest job tasks in a single request	Read	AgentSpace*		kms:Decrypt
BatchGetPentestJobs	Grants permission to retrieve multiple security testing jobs in a single request	Read	AgentSpace*		kms:Decrypt
BatchGetPentests	Grants permission to retrieve multiple penetration tests in a single request	Read	AgentSpace*		kms:Decrypt
BatchGetTargetDomains	Grants permission to retrieve multiple target domains in a single request	Read	TargetDomain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAgentSpace	Grants permission to create an agent space record	Write		aws:RequestTag/${TagKey} aws:TagKeys	kms:Decrypt kms:DescribeKey kms:GenerateDataKeyWithoutPlaintext
CreateApplication	Grants permission to create a new application	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole kms:DescribeKey sso:CreateApplication
CreateDesignReview	Grants permission to create a design review	Write	AgentSpace*		
CreateIntegration	Grants permission to create a security testing integration	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMembership	Grants permission to add a single member to a agent space with specified role	Write	AgentSpace*		
CreateOneTimeLoginSession	Grants permission to create a one time login session	Write	AgentSpace*		
CreatePentest	Grants permission to create a new penetration test configuration	Write	AgentSpace*		kms:Decrypt
CreateSecurityRequirement	Grants permission to add a customer managed Security Requirement	Write	SecurityRequirementPack*		
CreateTargetDomain	Grants permission to create a target domain record	Write			
DeleteAgentSpace	Grants permission to delete an agent space record	Write	AgentSpace*		kms:Decrypt
DeleteApplication	Grants permission to delete application	Write	Application*		
DeleteArtifact	Grants permission to delete an Artifact	Write	AgentSpace*		
DeleteDesignReview	Grants permission to delete a design review	Write	AgentSpace*		
DeleteIntegration	Grants permission to delete the integration of an application	Write	Integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMembership	Grants permission to remove a single member associated to an agent space	Write	AgentSpace*		
DeleteSecurityRequirement	Grants permission to delete a customer managed Security Requirement	Write	SecurityRequirementPack*		
DeleteTargetDomain	Grants permission to delete a target domain record	Write	TargetDomain*		
GetApplication	Grants permission to get application details by application ID	Read	Application*		
GetArtifact	Grants permission to retrieve an Artifact for the given Agent Space	Read	AgentSpace*		
GetDesignReview	Grants permission to get the status of the associated agent space design review	Read	AgentSpace*		
GetDesignReviewArtifact	Grants permission to get design review artifact for a specific document	Read	AgentSpace*		
GetDesignReviewFeedback	Grants permission to get feedback for a design review comment	Read	AgentSpace*		
GetIntegration	Grants permission to get the integration metadata by ID	Read	Integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSecurityRequirement	Grants permission to retrieve a Security Requirement	Read	SecurityRequirementPack*		
InitiateProviderRegistration	Grants permission to initiate the registration of Security Agent App for the given provider (eg: GitHub)	Write			
ListAgentSpaces	Grants permission to list agent spaces	List			
ListApplications	Grants permission to list all applications in the account	List			
ListArtifacts	Grants permission to list all artifacts for the given agent space	List	AgentSpace*		
ListDesignReviewComments	Grants permission to list design review comments	List	AgentSpace*		
ListDesignReviews	Grants permission to list all design reviews for the given agent space	List	AgentSpace*		
ListDiscoveredEndpoints	Grants permission to list discovered endpoints associated with a pentest job with optional URI prefix filtering	List	AgentSpace*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFindings	Grants permission to list findings with filtering and pagination support	List	AgentSpace*		kms:Decrypt
ListIntegratedResources	Grants permission to list integrated resources for an agent space	List	AgentSpace*		
ListIntegrations	Grants permission to get the integrations owned by the caller's AWS account	List			
ListMemberships	Grants permission to list all members associated to an agent space with pagination support	List	AgentSpace*		
ListPentestJobTasks	Grants permission to list pentest job tasks associated with a pentest job	List	AgentSpace*		kms:Decrypt
ListPentestJobsForPentest	Grants permission to list penetration test jobs associated with a penetration test	List	AgentSpace*		kms:Decrypt
ListPentests	Grants permission to list penetration tests with optional filtering by status	List	AgentSpace*		kms:Decrypt
ListResourcesFromIntegration	Grants permission to list resources from Integration	List	Integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSecurityRequirements	Grants permission to list all Security Requirements	List	SecurityRequirementPack*		
ListTagsForResource	Grants permission to list the tags for a resource	Read	AgentSpace		
			Application		
			Integration		
			SecurityRequirementPack		
			TargetDomain		
ListTargetDomains	Grants permission to list target domains	List			
PutDesignReviewFeedback	Grants permission to submit feedback for a design review comment	Write	AgentSpace*		
StartCodeRemediation	Grants permission to start code remediation for the findings	Write	AgentSpace*		kms:Decrypt kms:GenerateDataKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartPentestJob	Grants permission to initiate the execution of a penetration test	Write	AgentSpace*		kms:Decrypt kms:GenerateDataKey
StopPentestJob	Grants permission to stop the execution of a running penetration test	Write	AgentSpace*		kms:Decrypt
TagResource	Grants permission to add tags to a resource	Tagging	AgentSpace		
			Application		
			Integration		
			SecurityRequirementPack		
			TargetDomain		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ToggleManagedSecurityRequirement	Grants permission to toggle the status of a managed Security Requirement	Write	SecurityRequirementPack*		
UntagResource	Grants permission to remove tags from a resource	Tagging	AgentSpace		
			Application		
			Integration		
			SecurityRequirementPack		
			TargetDomain		
				aws:TagKeys	
UpdateAgentSpace	Grants permission to update an agent space record	Write	AgentSpace*		kms:Decrypt
UpdateApplication	Grants permission to update application configuration	Write	Application*		iam:PassRole kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFinding	Grants permission to update an existing security finding with new details or status	Write	AgentSpace*		kms:Decrypt
UpdateIntegratedResources	Grants permission to update integrated resources for an agent space	Write	AgentSpace*		
UpdatePentest	Grants permission to update an existing penetration test with new configuration or settings	Write	AgentSpace*		kms:Decrypt
UpdateSecurityRequirement	Grants permission to update a customer managed Security Requirement	Write	SecurityRequirementPack*		
UpdateTargetDomain	Grants permission to update a target domain record	Write	TargetDomain*		
VerifyTargetDomain	Grants permission to verify ownership for a registered target domain	Write	TargetDomain*		

Resource types defined by AWS Security Agent

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:${Partition}:securityagent:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
SecurityRequirementPack	arn:${Partition}:securityagent:${Region}:${Account}:security-requirement-pack/${SecurityRequirementPackId}	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:securityagent:${Region}:${Account}:integration/${IntegrationId}	aws:ResourceTag/${TagKey}
AgentSpace	arn:${Partition}:securityagent:${Region}:${Account}:agent-space/${AgentId}	aws:ResourceTag/${TagKey}
TargetDomain	arn:${Partition}:securityagent:${Region}:${Account}:target-domain/${TargetDomainId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Security Agent

AWS Security Agent defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Security Hub

AWS Security Hub (service prefix: `securityhub`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Security Hub
- Resource types defined by AWS Security Hub
- Condition keys for AWS Security Hub

Actions defined by AWS Security Hub

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAdministratorInvitation	Grants permission to accept Security Hub invitations to become a member account	Write	hub		
AcceptInvitation	Grants permission to accept Security Hub invitations to become a member account	Write	hub		
AllowVendedLogDeliveryForResource [permission only]	Grants permission to log delivery for resources	Permissions management	hub hubv2		
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*		
BatchGetConfigurat	Grants permission to retrieve information about configura	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ionPolicy Associations	tion policies associated with a specific list of member accounts and organizational units of the calling account's organization				
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateAutomationRules	Grants permission to update one or more automation rules from Security Hub based on rule Amazon Resource Names (ARNs) and input parameters	Write	automation-rule*		
BatchUpdateFindings	Grants permission to update customer-controlled fields for a selected set of Security Hub findings	Write	hub		
			hubv2		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath} securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	
BatchUpdateStandardsControlAssociations	Grants permission to update the enablement status of a batch of security controls in standards	Write			securityhub:UpdateStandardsControl
ConnectorRegistrationsV2	Grants permission to complete the OAuth 2.0 authorization code flow based on input parameters	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateActionTarget	Grants permission to create custom actions in Security Hub	Write	hub		
CreateAggregatorV2	Grants permission to create an aggregatorV2, which configures data aggregation across Regions	Write			
CreateAutomationRule	Grants permission to create an automation rule based on input parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomationRuleV2	Grants permission to create an automation rule V2 based on input parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	Grants permission to create a configuration policy to manage organization member settings in Security Hub	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnectorV2	Grants permission to create a connector V2 based on input parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	Grants permission to create a finding aggregator, which contains the cross-Region finding aggregation configuration	Write			
CreateInsight	Grants permission to create insights in Security Hub. Insights are collections of related findings	Write	hub		
CreateMembers	Grants permission to create member accounts in Security Hub	Write	hub		
CreateTicketV2	Grants permission to create ticket for a selected OCSF finding	Write	connectorv2		
DeclineInvitations	Grants permission to decline Security Hub invitations to become a member account	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteActionTarget	Grants permission to delete custom actions in Security Hub	Write	hub		
DeleteAggregatorV2	Grants permission to delete an aggregatorV2, which configures data aggregation across Regions	Write	aggregatorv2*		
DeleteAutomationRuleV2	Grants permission to delete an automation rule V2 in Security Hub	Write	automation-rulev2*		
DeleteConfigurationPolicy	Grants permission to delete an existing configuration policy	Write	configuration-policy*		
DeleteConnectorV2	Grants permission to delete a connector V2 in Security Hub	Write	connectorv2*		
DeleteFindingAggregator	Grants permission to delete a finding aggregator, which disables finding aggregation across Regions	Write	finding-aggregator*		
DeleteInsight	Grants permission to delete insights from Security Hub	Write	hub		
DeleteInvitations	Grants permission to delete Security Hub invitations to become a member account	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
DescribeProductsV2	Grants permission to retrieve information about the available Security Hub V2 product integrations	Read	hubv2		
DescribeSecurityHubV2	Grants permission to retrieve information about the hub V2 resource in your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStandards	Grants permission to retrieve information about Security Hub standards	Read	hub		
DescribeStandardsControls	Grants permission to retrieve information about Security Hub standards controls	Read	hub		
DisableImportFindingsForProduct	Grants permission to disable the findings importing for a Security Hub integrated product	Write	hub		
DisableOrganizationAdminAccount	Grants permission to remove the Security Hub administrator account for your organization	Write	hub		organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedAdministrators
DisableSecurityHub	Grants permission to disable Security Hub	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableSecurityHubV2	Grants permission to disable Security Hub V2	Write			
DisassociateFromAdministratorAccount	Grants permission to a Security Hub member account to disassociate from the associated administrator account	Write	hub		
DisassociateFromMasterAccount	Grants permission to a Security Hub member account to disassociate from the associated master account	Write	hub		
DisassociateMembers	Grants permission to disassociate Security Hub member accounts from the associated administrator account	Write	hub		
EnableImportFindingsForProduct	Grants permission to enable the findings importing for a Security Hub integrated product	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOrganizationAdminAccount	Grants permission to designate a Security Hub administrator account for your organization	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Grants permission to enable Security Hub	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableSecurityHubV2	Grants permission to enable Security Hub V2	Write		aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults [permission only]	Grants permission to retrieve aggregated statistical data about the findings	Read	hub		
			hubv2		
GetAdministratorAccount	Grants permission to retrieve details about the Security Hub administrator account	Read	hub		
GetAggregatorV2	Grants permission to retrieve details for an aggregatorV2, which configures data aggregation across Regions	Read	aggregatorv2*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAutomationRuleV2	Grants permission to retrieve details for an automation rule V2 from Security Hub based on rule Amazon Resource Name (ARN)	Read	automation-rulev2*		
GetConfigurationPolicy	Grants permission to get a complete overview of one configuration policy created by the calling account	Read	configuration-policy*		
GetConfigurationPolicyAssociation	Grants permission to retrieve information about a configuration policy associated with a member account or organizational unit of the calling account's organization	Read			
GetConnectorV2	Grants permission to retrieve details for a connector V2 from Security Hub based on connector id	Read	connectorv2*		
GetControlFindingSummary [permission only]	Grants permission to retrieve a security score and counts of finding and control statuses for a security standard	Read	hub		
GetEnabledStandards	Grants permission to retrieve a list of the standards that are enabled in Security Hub	List	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFindingAggregator	Grants permission to retrieve details for a finding aggregator, which configures finding aggregation across Regions	Read	finding-aggregator*		
GetFindingHistory	Grants permission to retrieve a list of finding history from Security Hub	Read	hub		
GetFindings	Grants permission to retrieve a list of findings from Security Hub	Read	hub		
			hubv2		
GetFindingsTrendsV2	Grants permission to retrieve findings trends	Read	hubv2		
GetFreeTrialEndDate [permission only]	Grants permission to retrieve the end date for an account's free trial of Security Hub	Read	hub		
GetFreeTrialUsage [permission only]	Grants permission to retrieve information about Security Hub usage during the free trial period	Read	hub		
GetInsightFindingTrend [permission only]	Grants permission to retrieve an insight finding trend from Security Hub in order to generate a graph	Read	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInsightResults	Grants permission to retrieve insight results from Security Hub	Read	hub		
GetInsights	Grants permission to retrieve Security Hub insights	List	hub		
GetInvitationsCount	Grants permission to retrieve the count of Security Hub membership invitations sent to the account	Read	hub		
GetMasterAccount	Grants permission to retrieve details about the Security Hub master account	Read	hub		
GetMembers	Grants permission to retrieve the details of Security Hub member accounts	Read	hub		
GetResourcesStatisticsV2	Grants permission to retrieve aggregate statistics about resources	Read	hubv2		
GetResourcesTrendsV2	Grants permission to retrieve resources trends	Read	hubv2		
GetResourcesV2	Grants permission to retrieve a list of resources	Read	hubv2		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSecurityControlDefinition	Grants permission to get the definition details of a specific security control identified by ID	Read			securityhub:DescribeStandardsControls
GetUsage [permission only]	Grants permission to retrieve information about Security Hub usage by accounts	Read	hub		
InviteMembers	Grants permission to invite other AWS accounts to become Security Hub member accounts	Write	hub		
ListAggregatorsV2	Grants permission to retrieve a list of aggregatorsV2, which configures data aggregation across Regions	List			
ListAutomationRules	Grants permission to retrieve a list of automation rules and their metadata for the calling account from Security Hub	List			
ListAutomationRulesV2	Grants permission to retrieve a list of automation rules V2 and their metadata for the calling account from Security Hub	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfigurationPolicies	Grants permission to list the summaries of all configuration policies created by the calling account	List			
ListConfigurationPolicyAssociations	Grants permission to retrieve information about all configuration policies associationed with all member accounts and organizational units of the calling account's organization	List			
ListConnectorsV2	Grants permission to retrieve a list of connectors V2 and their metadata for the calling account from Security Hub	List			
ListControlEvaluationSummaries [permission only]	Grants permission to retrieve a list of controls for a standard, including the control IDs, statuses and finding counts	Read	hub		
ListEnabledProductsForImport	Grants permission to retrieve the Security Hub integrated products that are currently enabled	List	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFindingAggregators	Grants permission to retrieve a list of finding aggregators, which contain the cross-Region finding aggregation configuration	List			
ListInvitations	Grants permission to retrieve the Security Hub invitations sent to the account	List	hub		
ListMembers	Grants permission to retrieve details about Security Hub member accounts associated with the administrator account	List	hub		
ListOrganizationAdminAccounts	Grants permission to list the Security Hub administrator accounts for your organization	List	hub		organizations:DescribeOrganization organizations:ListDelegatedAdministrators
ListSecurityControlDefinitions	Grants permission to retrieve a list of security control definitions, which contain details for security controls in the current region	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStandardsControlAssociations	Grants permission to list the enablement status of a security control in standards	List			securityhub:DescribeStandardsControls
ListTagsForResource	Grants permission to list of tags associated with a resource	Read	automation-rule		
			configuration-policy		
			hub		
SendFindingsEvents [permission only]	Grants permission to use a custom action to send Security Hub findings to Amazon EventBridge	Read	hub		
SendInsightEvents [permission only]	Grants permission to use a custom action to send Security Hub insights to Amazon EventBridge	Read	hub		
StartConfigurationPolicyAssociation	Grants permission to associate a configuration policy with a member account or organizational unit in the calling account's organization	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartConfiguration PolicyDisassociation	Grants permission to remove a configuration policy association from a member account or organizational unit in the calling account's organization	Write	hub		
TagResource	Grants permission to add tags to a Security Hub resource	Tagging	aggregatorv2		
			automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UntagResource	Grants permission to remove tags from a Security Hub resource	Tagging	aggregatorv2		
			automation-rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UpdateActionTarget	Grants permission to update custom actions in Security Hub	Write	hub		
UpdateAggregatorV2	Grants permission to update an aggregatorV2, which configures data aggregation across Regions	Write	aggregatorv2*		
UpdateAutomationRuleV2	Grants permission to update an automation rule V2 in Security Hub based on rule Amazon Resource Name (ARN) and input parameters	Write	automation-rulev2*		
UpdateConfigurationPolicy	Grants permission to update an existing configuration policy	Write	configuration-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnectorV2	Grants permission to update a connector V2 in Security Hub based on connector id and input parameters	Write	connectorv2*		
UpdateFindingAggregator	Grants permission to update a finding aggregator, which contains the cross-Region finding aggregation configuration	Write	finding-aggregator*		
UpdateFindings	Grants permission to update Security Hub findings	Write	hub		
UpdateInsight	Grants permission to update insights in Security Hub	Write	hub		
UpdateOrganizationConfiguration	Grants permission to update the organization configuration for Security Hub	Write	hub		
UpdateSecurityControl	Grants permission to update properties of a specific security control identified by ID or ARN	Write			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Grants permission to update Security Hub configuration	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStandardsControl	Grants permission to update Security Hub standards controls	Write	hub		

Resource types defined by AWS Security Hub

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
hub	`arn:${Partition}:securityhub:${Region}:${Account}:hub/default`	aws:ResourceTag/${TagKey}
hubv2	`arn:${Partition}:securityhub:${Region}:${Account}:hubv2/${HubV2Id}`	aws:ResourceTag/${TagKey}
product	`arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}`	
finding-aggregator	`arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}`	
aggregatorv2	`arn:${Partition}:securityhub:${Region}:${Account}:aggregatorv2/${AggregatorV2Id}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	aws:ResourceTag/${TagKey}
automation-rulev2	arn:${Partition}:securityhub:${Region}:${Account}:automation-rulev2/${AutomationRuleV2Id}	aws:ResourceTag/${TagKey}
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	aws:ResourceTag/${TagKey}
connectorv2	arn:${Partition}:securityhub:${Region}:${Account}:connectorv2/${ConnectorV2Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS Security Hub

AWS Security Hub defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filters access by the specified fields and values in the request	String
securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	Filters access by the specified fields and values in the request	String
securityhub:TargetAccount	Filters access by the AwsAccountId field that is specified in the request	String

Actions, resources, and condition keys for AWS Security Incident Response

AWS Security Incident Response (service prefix: `security-ir`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Security Incident Response
- Resource types defined by AWS Security Incident Response

- Condition keys for AWS Security Incident Response

Actions defined by AWS Security Incident Response

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetMemberAccountDetails	Grants permission to get member account details in batch	Read	membership*		
CancelMembership	Grants permission to cancel a membership	Write	membership*		
CloseCase	Grants permission to close a case	Write	case*		
CreateCase	Grants permission to create a case	Write	case*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCaseComment	Grants permission to create a case comment	Write	case*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMembership	Grants permission to create a membership	Write	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
GetCase	Grants permission to get a case	Read	case*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCaseAttachmentDownloadUrl	Grants permission to get a case attachment download URL	Read	case*		
GetCaseAttachmentUploadUrl	Grants permission to get a case attachment upload URL	Write	case*		
GetMembership	Grants permission to get a membership	Read	membership*		
ListCaseEdits	Grants permission to list case edits	Read	case*		
ListCases	Grants permission to list cases	List			
ListComments	Grants permission to list case comments	Read	case*		
ListInvestigations	Grants permission to list investigations for a case	Read	case*		
ListMemberships	Grants permission to list memberships	List			
ListTagsForResource	Grants permission to list the tags attached to the specified resource	Read	case membership		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
SendFeedback	Grants permission to send feedback for investigation results	Write	case*		
TagResource	Grants permission to add tags to the specified resource	Tagging	case		
			membership		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	case		
			membership		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCase	Grants permission to update a case	Write	case*		
UpdateCaseComment	Grants permission to update a case comment	Write	case*		
UpdateCaseStatus	Grants permission to update a case status	Write	case*		
UpdateMembership	Grants permission to update memberships	Write	membership*		iam:CreateServiceLinkedRole organizations:DescribeOrganizationalUnit
UpdateResolverType	Grants permission to update case resolver type	Write	case*		

Resource types defined by AWS Security Incident Response

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
case	`arn:${Partition}:security-ir:${Region}:${Account}:case/${CaseId}`	aws:ResourceTag/${TagKey}
membership	`arn:${Partition}:security-ir:${Region}:${Account}:membership/${MembershipId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Security Incident Response

AWS Security Incident Response defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Security Lake

Amazon Security Lake (service prefix: `securitylake`) 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 Lake

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAwsLogSource	Grants permission to enable any source type in any region for accounts that are either	Write	data-lake*		glue:CreateDatabase

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	part of a trusted organization or standalone account				glue:CreateTable glue:GetDatabase glue:GetTable iam:CreateServiceLinkedRole kms:CreateGrant kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomLogSource	Grants permission to add a custom source	Write	data-lake*		glue:CreateCrawler glue:CreateDatabase glue:CreateTable glue:StartCrawlerSchedule iam:DeleteRolePolicy iam:GetRole iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:GenerateDataKey lakeformation:GrantPermissions lakeformation:RegisterResource s3:ListBucket s3:PutObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataLake	Grants permission to create a new security data lake	Write	data-lake *		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PassRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetD

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ataLakeSettings lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListAccounts organizations:ListDelegatedServicesF

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					orAccount s3:CreateBucket s3:GetObject s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					sqs:SetQueueAttributes
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeExceptionSubscription	Grants permission to get instant notifications about exceptions. Subscribes to the SNS topics for exception notifications	Write			
CreateDataLakeOrganizationConfiguration	Grants permission to automatically enable Amazon Security Lake for new member accounts in your organization	Write	data-lake*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubscriber	Grants permission to create a subscriber	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:CreateRole iam:DeleteRolePolicy iam:GetRole iam:PutRolePolicy lakeformation:GrantPermissions lakeformation:ListPermissions lakeformation:RegisterResource lakeformation:RevokePermissions

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ram:GetResourceShareAssociations ram:GetResourceShares ram:UpdateResourceShare s3:PutObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubscriberNotification	Grants permission to create a webhook invocation to notify a client when there is new data in the data lake	Write	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PassRole s3:GetBucketNotification s3:PutBucketNotification sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes
DeleteAwsLogSource	Grants permission to disable any source type in any region for accounts that are part of a trusted organization or standalone accounts	Write	data-lake*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomLogSource	Grants permission to remove a custom source	Write	data-lake*		glue:StopCrawlerSchedule
DeleteDataLake	Grants permission to delete security data lake	Write	data-lake*		organizations:DescribeOrganization organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount
DeleteDataLakeExceptionSubscription	Grants permission to unsubscribe from SNS topics for exception notifications. Removes exception notifications for the SNS topic	Write			
DeleteDataLakeOrganizationConfiguration	Grants permission to remove the automatic enablement of Amazon Security Lake access for new organization accounts	Write	data-lake*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubscriber	Grants permission to delete the specified subscriber	Write	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:GetRole iam:ListRolePolicies lakeformation:ListPermissions lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubscriberNotification	Grants permission to remove a webhook invocation to notify a client when there is new data in the data lake	Write	subscriber*		events:DeleteApiDestination events:DeleteConnection events:DeleteRule events:DescribeRule events:ListApiDestinations events:ListTargetsByRule events:RemoveTargets iam:DeleteRole iam:DeleteRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:GetRole iam:ListRolePolicies lakeformation:RevokePermissions sqs:DeleteQueue sqs:GetQueueUrl
DeregisterDataLakeDelegatedAdministrator	Grants permission to remove the Delegated Administrator account and disable Amazon Security Lake as a service for this organization	Write			organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataLakeExceptionSubscription	Grants permission to query the protocol and endpoint that were provided when subscribing to SNS topics for exception notifications	Read			
GetDataLakeOrganizationConfiguration	Grants permission to get an organization's configuration setting for automatically enabling Amazon Security Lake access for new organization accounts	Read	data-lake*		organizations:DescribeOrganization
GetDataLakeSources	Grants permission to get a static snapshot of the security data lake in the current region. The snapshot includes enabled accounts and log sources	Read	data-lake*		
GetSubscriber	Grants permission to get information about subscriber that is already created	Read	subscriber*		
ListDataLakeExceptions	Grants permission to get the list of all non-retryable failures	List			
ListDataLakes	Grants permission to list information about the security data lakes	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLogSources	Grants permission to view the enabled accounts. You can view the enabled sources in the enabled regions	List			
ListSubscribers	Grants permission to list all subscribers	List			
ListTagsForResource	Grants permission to list all tags for the resource	List	data-lake		
			subscriber		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterDataLakeDelegatedAdministrator	Grants permission to designate an account as the Amazon Security Lake administrator account for the organization	Write			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators organizations:ListDelegatedServicesForAccount organizations:RegisterDelegatedAdministrator

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to the resource	Tagging	data-lake		
			subscriber		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from the resource	Tagging	data-lake		
			subscriber		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataLake	Grants permission to update a security data lake	Write	data-lake*		events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:PutRolePolicy kms:CreateGrant kms:DescribeKey lakeformation:GetDataLakeSettings

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					lakeformation:PutDataLakeSettings lambda:AddPermission lambda:CreateEventSourceMapping lambda:CreateFunction organizations:DescribeOrganization organizations:ListDelegatedServicesForAccount s3:CreateBucket s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetObjectVersion s3:ListBucket s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning sqs:CreateQueue sqs:GetQueueAttributes sqs:SetQueueAttributes
UpdateDataLakeExceptionSubscription	Grants permission to update subscriptions to the SNS topics for exception notifications	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSubscriber	Grants permission to update subscriber	Write	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:DeleteRolePolicy iam:GetRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PutRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSubscriberNotification	Grants permission to update a webhook invocation to notify a client when there is new data in the data lake	Write	subscriber*		events:CreateApiDestination events:CreateConnection events:DescribeRule events:ListApiDestinations events:ListConnections events:PutRule events:PutTargets iam:CreateServiceLinkedRole iam:DeleteRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:GetRole iam:PassRole iam:PutRolePolicy s3:CreateBucket s3:GetBucketNotification s3:ListBucket s3:PutBucketNotification s3:PutBucketPolicy s3:PutBucketPublicAccessBlock s3:PutBucketVersioning

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:PutLifecycleConfiguration sqs:CreateQueue sqs:DeleteQueue sqs:GetQueueAttributes sqs:GetQueueUrl sqs:SetQueueAttributes

Resource types defined by Amazon Security Lake

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
data-lake	arn:${Partition}:securitylake:${Region}:${Account}:data-lake/default	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}
subscriber	arn:${Partition}:securitylake:${Region}:${Account}:subscriber/${SubscriberId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Condition keys for Amazon Security Lake

Amazon Security Lake defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Security Token Service

AWS Security Token Service (service prefix: `sts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Security Token Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRole	Grants permission to obtain a set of temporary security credentials that you can use to access AWS resources that you might not normally have access to	Write	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sts:TransitiveTagKeys sts:ExternalId sts:RoleSessionName iam:ResourceTag/${TagKey} sts:SourceIdentity cognito-identity.amazonaws.com:amr cognito-identity.amazonaws.com:aud cognito-identity.amazonaws.com:sub	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 saml:namequalifier saml:sub saml:sub_type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoleWithSAML	Grants permission to obtain a set of temporary security credentials for users who have been authenticated via a SAML authentication response	Write	role*		
				saml:namequalifier saml:sub saml:sub_type saml:aud saml:iss saml:doc saml:cn saml:commonName saml:eduorghomepageuri saml:eduorgidentityauthnpolicyuri saml:eduorglegalname	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				saml:eduorgsuperioruri saml:eduorgwhitepagesuri saml:edupersonaffiliation saml:edupersonassurance saml:edupersonentitlement saml:edupersonnickname saml:edupersonorgdn saml:edupersonorgunitdn saml:edupersonprim	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aryaffiliation saml:edupersonprimaryorgunitdn saml:edupersonprincipalname saml:edupersonscopedaffiliation saml:edupersontargetedid saml:givenName saml:mail saml:name saml:organizationStatus saml:primaryGroupSID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				saml:surname saml:uid saml:x500UniqueIdentifier aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:SourceIdentity sts:RoleSessionName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoleWithWebIdentity	Grants permission to obtain a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider	Write	role*		
				cognito-identity.amazonaws.com:amr cognito-identity.amazonaws.com:aud cognito-identity.amazonaws.com:sub www.amazon.com:app_id www.amazon.com:user_id graph.facebook.com:app_id graph.facebook.com:id	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				accounts.google.com:aud accounts.google.com:oaud accounts.google.com:sub aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:SourceIdentity sts:RoleSessionName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoot	Grants permission to obtain a set of temporary security credentials that you can use to perform privileged tasks in member accounts in your organization	Write	root-user *		
				sts:TaskPolicyArn	
DecodeAuthorizationMessage	Grants permission to decode additional information about the authorization status of a request from an encoded message returned in response to an AWS request	Write			
GetAccessKeyInfo	Grants permission to obtain details about the access key id passed as a parameter to the request	Read			
GetCallerIdentity	Grants permission to obtain details about the IAM identity whose credentials are used to call the API	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDelegatedAccessToken	Returns temporary security credentials for accessing an AWS account after temporary delegation request approval. This API requires the tradeInToken provided upon request delegation approval and is intended to be used only by Amazon or AWS Partners	Write			
GetFederationToken	Grants permission to obtain a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for a federated user	Read	federated-user		
			user		
				aws:TagKeys aws:RequestTag/${TagKey}	
GetServiceBearerToken [permission only]	Grants permission to obtain a STS bearer token for an AWS root user, IAM role, or an IAM user	Read		sts:AWSServiceName sts:DurationSeconds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSessionToken	Grants permission to obtain a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for an AWS account or IAM user	Read			
GetWebIdentityToken	Grants permission to obtain a short-lived, publicly verifiable JSON Web Token (JWT) that represents the calling IAM principal's identity	Write		sts:DurationSeconds sts:IdentityTokenAudience sts:SigningAlgorithm aws:TagKeys aws:RequestTag/${TagKey}	
SetContext [permission only]	Grants permission to set context keys on a STS session	Write	role self-session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sts:RequestContext/${ContextKey} sts:RequestContextProviders	
SetSourceIdentity [permission only]	Grants permission to set a source identity on a STS session	Write	role		
			user		
				sts:SourceIdentity	
TagGetWebIdentityToken [permission only]	Grants permission to add tags to the JSON Web Token (JWT) generated by the GetWebIdentityToken API	Tagging		aws:TagKeys aws:RequestTag/${TagKey}	
TagSession [permission only]	Grants permission to add tags to a STS session	Tagging	role		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys saml:aud	

Resource types defined by AWS Security Token Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
role	`arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	
root-user	arn:${Partition}:iam::${Account}:root	
self-session	arn:${Partition}:sts::${Account}:self	
context-provider	arn:${Partition}:iam::aws:contextProvider/${ContextProviderName}	
federated-user	arn:${Partition}:sts::${Account}:federated-user/${FederatedUserName}	

Condition keys for AWS Security Token Service

AWS Security Token Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
accounts.google.com:aud	Filters access by the Google application ID	String
accounts.google.com:oaud	Filters access by the Google audience	String
accounts.google.com:sub	Filters access by the subject of the claim (the Google user ID)	String

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
cognito-identity.amazonaws.com:amr	Filters access by the login information for Amazon Cognito	String
cognito-identity.amazonaws.com:aud	Filters access by the Amazon Cognito identity pool ID	String
cognito-identity.amazonaws.com:sub	Filters access by the subject of the claim (the Amazon Cognito user ID)	String
graph.facebook.com:app_id	Filters access by the Facebook application ID	String
graph.facebook.com:id	Filters access by the Facebook user ID	String
iam:ResourceTag/${TagKey}	Filters access by the tags that are attached to the role that is being assumed	String

Condition keys	Description	Type
saml:aud	Filters access by the endpoint URL to which SAML assertions are presented	String
saml:cn	Filters access by the eduOrg attribute	ArrayOfString
saml:commonName	Filters access by the commonName attribute	String
saml:doc	Filters access by on the principal that was used to assume the role	String
saml:eduorghomepageuri	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorgidentityauthnpolicyuri	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorglegalname	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorgsuperioruri	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorgwhitepagesuri	Filters access by the eduOrg attribute	ArrayOfString
saml:edupersonaffiliation	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonassurance	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonentitlement	Filters access by the eduPerson attribute	ArrayOfString

Condition keys	Description	Type
saml:edupersonnickname	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonorgdn	Filters access by the eduPerson attribute	String
saml:edupersonorgunitdn	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonprimaryaffiliation	Filters access by the eduPerson attribute	String
saml:edupersonprimaryorgunitdn	Filters access by the eduPerson attribute	String
saml:edupersonprincipalname	Filters access by the eduPerson attribute	String
saml:edupersonscopedaffiliation	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersontargetedid	Filters access by the eduPerson attribute	ArrayOfString
saml:givenName	Filters access by the givenName attribute	String
saml:iss	Filters access by on the issuer, which is represented by a URN	String
saml:mail	Filters access by the mail attribute	String
saml:name	Filters access by the name attribute	String

Condition keys	Description	Type
saml:name qualifier	Filters access by the hash value of the issuer, account ID, and friendly name	String
saml:orga nizationStatus	Filters access by the organizationStatus attribute	String
saml:prim aryGroupSID	Filters access by the primaryGroupSID attribute	String
saml:sub	Filters access by the subject of the claim (the SAML user ID)	String
saml:sub_type	Filters access by the value persistent, transient, or the full Format URI	String
saml:surname	Filters access by the surname attribute	String
saml:uid	Filters access by the uid attribute	String
saml:x500 UniqueIdentifier	Filters access by the uid attribute	String
sts:AWSSe rviceName	Filters access by the service that is obtaining a bearer token	String
sts:Durat ionSeconds	Filters access by the duration in seconds when getting a bearer token or a JSON Web Token (JWT) from the GetWebIdentityToken API	Numeric
sts:ExternalId	Filters access by the unique identifier required when you assume a role in another account	String
sts:Ident ityTokenA udience	Filters access by the audience that is passed in the request	ArrayOfString

Condition keys	Description	Type
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
sts:RequestContextProviders	Filters access by the context provider ARNs	ArrayOfARN
sts:RoleSessionName	Filters access by the role session name required when you assume a role	String
sts:SigningAlgorithm	Filters access by the signing algorithm that is passed in the request	String
sts:SourceIdentity	Filters access by the source identity that is passed in the request	String
sts:TaskPolicyArn	Filters access by TaskPolicyARN	String
sts:TransitiveTagKeys	Filters access by the transitive tag keys that are passed in the request	ArrayOfString
www.amazon.com:app_id	Filters access by the Login with Amazon application ID	String
www.amazon.com:user_id	Filters access by the Login with Amazon user ID	String

Actions, resources, and condition keys for AWS Server Migration Service

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApp	Grants permission to create an application configuration to migrate on-premise application onto AWS	Write			
CreateReplicationJob	Grants permission to create a job to migrate on-premise server onto AWS	Write			
DeleteApp	Grants permission to delete an existing application configuration	Write			
DeleteAppLaunchConfiguration	Grants permission to delete launch configuration for an existing application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAppReplicationConfiguration	Grants permission to delete replication configuration for an existing application	Write			
DeleteAppValidationConfiguration	Grants permission to delete validation configuration for an existing application	Write			
DeleteReplicationJob	Grants permission to delete an existing job to migrate on-premise server onto AWS	Write			
DeleteServerCatalog	Grants permission to delete the complete list of on-premise servers gathered into AWS	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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 AWS Server Migration Service to Server Migration Connector	Read			
GetReplicationJobs	Grants permission to get all existing jobs to migrate on-premise servers onto AWS	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReplicationRuns	Grants permission to get all runs for an existing job	Read			
GetServers	Grants permission to get all servers that have been imported	Read			
ImportAppCatalog	Grants permission to import application catalog from AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAppReplicationConfiguration	Grants permission to create or update replication configuration for an existing application	Write			
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 AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TerminateApp	Grants permission to terminate the CloudFormation stack for an existing application	Write			
UpdateApp	Grants permission to update an existing application configuration	Write			
UpdateReplicationJob	Grants permission to update an existing job to migrate on-premise server onto AWS	Write			

Resource types defined by AWS Server Migration Service

AWS Server Migration Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Server Migration Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Serverless Application Repository

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an application, optionally including an AWS 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 AWS CloudFormation ChangeSet for the given application	Write	applications*		
				serverlessrepo:applicationType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCloudFormationTemplate	Grants permission to create an AWS CloudFormation template	Write	applications*		
				serverlessrepo:applicationType	
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 AWS CloudFormation template	Read	applications*		
ListApplicationDependencies	Grants permission to retrieve the list of applications nested in the containing application	List	applications*		
				serverlessrepo:applicationType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplicationVersions	Grants permission to list versions for the specified application owned by the requester	List	applications*		
				serverlessrepo:applicationType	
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 AWS 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 AWS Serverless Application Repository

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
serverlessrepo:applicationType	Filters access by application type	String

Actions, resources, and condition keys for AWS Service - Oracle Database@AWS

AWS Service - Oracle Database@AWS (service prefix: odb) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Service - Oracle Database@AWS

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptMarketplaceRegistration	Grants permission to register the Amazon Web Services Marketplace token for your Amazon Web Services account to activate your Oracle Database@Amazon Web Services subscription	Write			
CreateCloudAutonomousVmCluster	Grants permission to create a new Autonomous VM cluster in the specified Exadata infrastructure	Write	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateCloudExadataInfrastructure	Grants permission to create an Exadata infrastructure	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudVmCluster	Grants permission to create a VM cluster on the specified Exadata infrastructure	Write	cloud-exadata-infrastructure*		
			odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbNode [permission only]	Grants permission to create a DB Node	Write	db-node*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGrantShare [permission only]	Grants permission to create an ODB Grant Share	Write			
CreateOdbNetwork	Grants permission to create an ODB network	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOdbPeeringConnection	Grants permission to create an ODB Peering Connection	Write	odb-network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutboundIntegration [permission only]	Grants permission to create an Outbound Integration	Write	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCloudAutonomousVmCluster	Grants permission to Deletes an Autonomous VM cluster	Write	cloud-autonomous-vm-cluster*		
DeleteCloudExadataInfrastructure	Grants permission to delete a specified Exadata infrastructure. Before you use this operation, make sure to delete all of the VM clusters that are hosted on this Exadata infrastructure	Write	cloud-exadata-infrastructure*		
DeleteCloudVmCluster	Grants permission to delete a specified VM cluster	Write	cloud-vm-cluster*		
DeleteDbNode [permission only]	Grants permission to delete a DB Node	Write	db-node*		
DeleteGrantShare [permission only]	Grants permission to delete an ODB Grant Share	Write			
DeleteOdbNetwork	Grants permission to delete the specified ODB network	Write	odb-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOdbPeeringConnection	Grants permission to delete the specified ODB Peering Connection. When you delete an ODB peering connection, the underlying VPC peering connection is also deleted	Write	odb-peering-connection*		
DeleteResourcePolicy [permission only]	Grants permission to delete a resource policy	Write	cloud-exadata-infrastructure*		
			odb-network*		
GetCloudAutonomousVmCluster	Grants permission to get information about a specific Autonomous VM cluster	Read	cloud-autonomous-vm-cluster*		
GetCloudExadataInfrastructure	Grants permission to get information about the specified Exadata infrastructure	Read	cloud-exadata-infrastructure*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCloudExadataInfrastructureUnallocatedResources	Grants permission to retrieve information about unallocated resources in a specified Cloud Exadata Infrastructure	Read	cloud-exadata-infrastructure*		
GetCloudVmCluster	Grants permission to get information about the specified VM cluster	Read	cloud-vm-cluster*		
GetDbNode	Grants permission to get information about the specified DB node	Read	cloud-vm-cluster*		
			db-node*		
GetDbServer	Grants permission to get information about the specified database server	Read	cloud-exadata-infrastructure*		
GetOciOnboardingStatus	Grants permission to get the tenancy activation link and onboarding status for your Amazon Web Services account	Read			
GetOdbNetwork	Grants permission to get information about the specified ODB network	Read	odb-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOdbPeeringConnection	Grants permission to get information about the specified ODB Peering connection	Read	odb-peering-connection*		
GetResourcePolicy [permission only]	Grants permission to get a resource policy	Read	cloud-exadata-infrastructure*		
			odb-network*		
InitializeService	Grants permission to initialize the ODB service for the first time in an account	Write			
ListAutonomousVirtualMachines	Grants permission to list all Autonomous VMs in an Autonomous VM cluster	Read	cloud-autonomous-vm-cluster		
ListCloudAutonomousVmClusters	Grants permission to list all Autonomous VM clusters in a specified Cloud Exadata infrastructure	List	cloud-exadata-infrastructure		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCloudExadataInfrastructures	Grants permission to list information about the Exadata infrastructures owned by your Amazon Web Services account	List			
ListCloudVmClusters	Grants permission to list information about the VM clusters owned by your Amazon Web Services account or only the ones on the specified Exadata infrastructure	List	cloud-exadata-infrastructure		
ListDbNodes	Grants permission to list information about the DB nodes for the specified VM cluster	List	cloud-vm-cluster*		
ListDbServers	Grants permission to list information about the database servers that belong to the specified Exadata infrastructure	Read	cloud-exadata-infrastructure*		
ListDbSystemShapes	Grants permission to list information about the shapes that are available for an Exadata infrastructure	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGiVersions	Grants permission to list information about Oracle Grid Infrastructure (GI) software versions that are available for a VM cluster for the specified shape	Read			
ListOdbNetworks	Grants permission to list information about the ODB networks owned by your Amazon Web Services account	List			
ListOdbPeeringConnections	Grants permission to list all ODB peering connections or those associated with a specific ODB network	List	odb-network		
ListSystemVersions	Grants permission to list information about the system versions that are available for a VM cluster for the specified giVersion and shape	Read			
ListTagsForResource	Grants permission to list information about the tags applied to this resource	Read	cloud-autonomous-vm-cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey}	
PutResourcePolicy [permission only]	Grants permission to update a resource policy	Write	cloud-exadata-infrastructure*		
			odb-network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RebootDbNode	Grants permission to reboot the specified DB node in a VM cluster	Write	cloud-vm-cluster*		
			db-node*		
StartDbNode	Grants permission to start the specified DB node in a VM cluster	Write	cloud-vm-cluster*		
			db-node*		
StopDbNode	Grants permission to stop the specified DB node in a VM cluster	Write	cloud-vm-cluster*		
TagResource	Grants permission to apply tags to the specified resource	Tagging	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		
			cloud-vm-cluster		
			db-node		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			odb-network		
			odb-peering-connection		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	cloud-autonomous-vm-cluster		
			cloud-exadata-infrastructure		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cloud-vm-cluster		
			db-node		
			odb-network		
			odb-peering-connection		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCloudExadataInfrastructure	Grants permission to update the properties of an Exadata infrastructure resource	Write	cloud-exadata-infrastructure*		
UpdateGrantShare [permission only]	Grants permission to update an ODB Grant Share	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOdbNetwork	Grants permission to update properties of a specified ODB network	Write	odb-network*		
UpdateOdbPeeringConnection	Grants permission to update properties of a specified ODB Peering Connection	Write	odb-peering-connection*		
UpdateOutboundIntegration [permission only]	Grants permission to update an Outbound Integration	Write	cloud-autonomous-vm-cluster*		
			cloud-vm-cluster*		

Resource types defined by AWS Service - Oracle Database@AWS

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
cloud-autonomous-vm-cluster	arn:${Partition}:odb:${Region}:${Account}:cloud-autonomous-vm-cluster/${CloudAutonomousVmClusterId}	aws:ResourceTag/${TagKey}
cloud-exadata-infrastructure	arn:${Partition}:odb:${Region}:${Account}:cloud-exadata-infrastructure/${CloudExadataInfrastructureId}	aws:ResourceTag/${TagKey}
cloud-vm-cluster	arn:${Partition}:odb:${Region}:${Account}:cloud-vm-cluster/${CloudVmClusterId}	aws:ResourceTag/${TagKey}
db-node	arn:${Partition}:odb:${Region}:${Account}:db-node/${DbNodeId}	aws:ResourceTag/${TagKey}
odb-network	arn:${Partition}:odb:${Region}:${Account}:odb-network/${OdbNetworkId}	aws:ResourceTag/${TagKey}
odb-peering-connection	arn:${Partition}:odb:${Region}:${Account}:odb-peering-connection/${OdbPeeringConnectionId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Service - Oracle Database@AWS

AWS Service - Oracle Database@AWS defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Service Catalog

AWS Service Catalog (service prefix: `servicecatalog`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Service Catalog
- Resource types defined by AWS Service Catalog
- Condition keys for AWS Service Catalog

Actions defined by AWS Service Catalog

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptPortfolioShare	Grants permission to accept a portfolio that has been shared with you	Write	Portfolio*		
AssociateAttributeGroup	Grants permission to associate an attribute group with an application	Write	Application* AttributeGroup*		
AssociateBudgetWithResource	Grants permission to associate a budget with a resource	Write			
AssociatePrincipalWithPortfolio	Grants permission to associate an IAM principal with a portfolio, giving the specified principal access to any products associated with the specified portfolio	Write	Portfolio*		
AssociateProductWithPortfolio	Grants permission to associate a product with a portfolio	Write			
AssociateResource	Grants permission to associate a resource with an application	Write	Application*		cloudformation:DescribeStacks resource-groups:CreateGroup

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					resource-groups:GetGroup resource-groups:Tag
				servicecatalog:ResourceType servicecatalog:Resource	
AssociateServiceActionWithProvisioningArtifact	Grants permission to associate an action with a provisioning artifact	Write	Product*		
AssociateTagOptionWithResource	Grants permission to associate the specified TagOption with the specified portfolio or product	Write	Portfolio Product		
BatchAssociateServiceActionWithProvisioningArtifact	Grants permission to associate multiple self-service actions with provisioning artifacts	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDisassociateServiceActionFromProvisioningArtifact	Grants permission to disassociate a batch of self-service actions from the specified provisioning artifact	Write			
CopyProduct	Grants permission to copy the specified source product to the specified target product or a new product	Write			
CreateApplication	Grants permission to create an application	Write	Application*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAttributeGroup	Grants permission to create an attribute group	Write	AttributeGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConstraint	Grants permission to create a constraint on an associated product and portfolio	Write	Product*		
CreatePortfolio	Grants permission to create a portfolio	Write	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePortfolioShare	Grants permission to share a portfolio you own with another AWS account	Permissions management	Portfolio*		
CreateProduct	Grants permission to create a product and that product's first provisioning artifact	Write	Product*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedProductPlan	Grants permission to add a new provisioned product plan	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
CreateProvisioningArtifact	Grants permission to add a new provisioning artifact to an existing product	Write	Product*		
CreateServiceAction	Grants permission to create a self-service action	Write			
CreateTagOption	Grants permission to create a TagOption	Write			
DeleteApplication	Grants permission to delete an application if all associations have been removed from the application	Write	Application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAttributeGroup	Grants permission to delete an attribute group if all associations have been removed from the attribute group	Write	AttributeGroup*		
DeleteConstraint	Grants permission to remove and delete an existing constraint from an associated product and portfolio	Write			
DeletePortfolio	Grants permission to delete a portfolio if all associations and shares have been removed from the portfolio	Write	Portfolio*		
DeletePortfolioShare	Grants permission to unshare a portfolio you own from an AWS account you previously shared the portfolio with	Permissions management	Portfolio*		
DeleteProduct	Grants permission to delete a product if all associations have been removed from the product	Write	Product*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProvisionedProductPlan	Grants permission to delete a provisioned product plan	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DeleteProvisioningArtifact	Grants permission to delete a provisioning artifact from a product	Write	Product*		
DeleteResourcePolicy [permission only]	Grants permission to delete a resource-based policy for the specified resource	Write	Application		
			AttributeGroup		
DeleteServiceAction	Grants permission to delete a self-service action	Write			
DeleteTagOption	Grants permission to delete the specified TagOption	Write			
DescribeConstraint	Grants permission to describe a constraint	Read			
DescribeCopyProductStatus	Grants permission to get the status of the specified copy product operation	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePortfolio	Grants permission to describe a portfolio	Read	Portfolio*		
DescribePortfolioShareStatus	Grants permission to get the status of the specified portfolio share operation	Read			
DescribePortfolioShares	Grants permission to view a summary of each of the portfolio shares that were created for the specified portfolio	List	Portfolio*		
DescribeProduct	Grants permission to describe a product as an end-user	Read	Product*		
DescribeProductAsAdmin	Grants permission to describe a product as an admin	Read	Product*		
DescribeProductView	Grants permission to describe a product as an end-user	Read			
DescribeProvisionedProduct	Grants permission to describe a provisioned product	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProvisionedProductPlan	Grants permission to describe a provisioned product plan	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeProvisioningArtifact	Grants permission to describe a provisioning artifact	Read	Product*		
DescribeProvisioningParameters	Grants permission to describe the parameters that you need to specify to successfully provision a specified provisioning artifact	Read	Product*		
DescribeRecord	Grants permission to describe a record and lists any outputs	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServiceAction	Grants permission to describe a self-service action	Read			
DescribeServiceActionExecutionParameters	Grants permission to get the default parameters if you executed the specified Service Action on the specified Provisioned Product	Read		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
DescribeTagOption	Grants permission to get information about the specified TagOption	Read			
DisableAWSOrganizationsAccess	Grants permission to disable portfolio sharing through AWS Organizations feature	Write			
DisassociateAttributeGroup	Grants permission to disassociate an attribute group from an application	Write	Application* AttributeGroup*		
DisassociateBudgetFromResource	Grants permission to disassociate a budget from a resource	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociatePrincipalFromPortfolio	Grants permission to disassociate an IAM principal from a portfolio	Write	Portfolio*		
DisassociateProductFromPortfolio	Grants permission to disassociate a product from a portfolio	Write			
DisassociateResource	Grants permission to disassociate a resource from an application	Write	Application*		resource-groups:DeleteGroup
				servicecatalog:ResourceType servicecatalog:Resource	
DisassociateServiceActionFromProvisioningArtifact	Grants permission to disassociate the specified self-service action association from the specified provisioning artifact	Write	Product*		
DisassociateTagOptionFromResource	Grants permission to disassociate the specified TagOption from the specified resource	Write	Portfolio		
			Product		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableAWSOrganizationsAccess	Grants permission to enable portfolio sharing feature through AWS Organizations	Write			
ExecuteProvisionedProductPlan	Grants permission to execute a provisioned product plan	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ExecuteProvisionedProductServiceAction	Grants permission to executes a provisioned product plan	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
GetAWSOrganizationsAccessStatus	Grants permission to get the access status of AWS Organization portfolio share feature	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApplication	Grants permission to get an application	Read	Application*		
GetAssociatedResource	Grants permission to get information about a resource associated to an application	Read	Application*		
				servicecatalog:ResourceType servicecatalog:Resource	
GetAttributeGroup	Grants permission to get an attribute group	Read	AttributeGroup*		
GetConfiguration	Grants permission to read AppRegistry configurations	Read			
GetProvisionedProductOutputs	Grants permission to get the provisioned product output with either provisioned product id or name	Read			
GetResourcePolicy [permission only]	Grants permission to get a resource-based policy for the specified resource	Read	Application		
			AttributeGroup		
ImportAsProvisionedProduct	Grants permission to import a resource into a provisioned product	Write	Product*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAcceptedPortfolioShares	Grants permission to list the portfolios that have been shared with you and you have accepted	List			
ListApplications	Grants permission to list your applications	List			
ListAssociatedAttributeGroups	Grants permission to list the attribute groups associated with an application	List	Application*		
ListAssociatedResources	Grants permission to list the resources associated with an application	List	Application*		
ListAttributeGroups	Grants permission to list your attribute groups	List			
ListAttributeGroupsForApplication	Grants permission to list the associated attribute groups for a given application	List	Application*		
ListBudgetsForResource	Grants permission to list all the budgets associated to a resource	List			
ListConstraintsForPortfolio	Grants permission to list constraints associated with a given portfolio	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLaunchPaths	Grants permission to list the different ways to launch a given product as an end-user	List	Product*		
ListOrganizationPortfolioAccess	Grants permission to list the organization nodes that have access to the specified portfolio	List			
ListPortfolioAccess	Grants permission to list the AWS accounts you have shared a given portfolio with	List	Portfolio*		
ListPortfolios	Grants permission to list the portfolios in your account	List			
ListPortfoliosForProduct	Grants permission to list the portfolios associated with a given product	List	Product*		
ListPrincipalsForPortfolio	Grants permission to list the IAM principals associated with a given portfolio	List	Portfolio*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProvisionedProductPlans	Grants permission to list the provisioned product plans	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListProvisioningArtifacts	Grants permission to list the provisioning artifacts associated with a given product	List	Product*		
ListProvisioningArtifactsForServiceAction	Grants permission to list all provisioning artifacts for the specified self-service action	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecordHistory	Grants permission to list all the records in your account or all the records related to a given provisioned product	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListResourcesForTagOption	Grants permission to list the resources associated with the specified TagOption	List			
ListServiceActions	Grants permission to list all self-service actions	List			
ListServiceActionsForProvisioningArtifact	Grants permission to list all the service actions associated with the specified provisioning artifact in your account	List	Product*		
				servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStackInstancesForProvisionedProduct	Grants permission to list account, region and status of each stack instances that are associated with a CFN_STACKSET type provisioned product	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
ListTagOptions	Grants permission to list the specified TagOptions or all TagOptions	List			
ListTagsForResource	Grants permission to list the tags for a service catalog appregistry resource	Read	Application		
			AttributeGroup		
NotifyProvisionProductEngineWorkflowResult	Grants permission to notify the result of the provisioning engine execution	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyTerminateProvisionedProductEngineWorkflowResult	Grants permission to notify the result of the terminate engine execution	Write			
NotifyUpdateProvisionedProductEngineWorkflowResult	Grants permission to notify the result of the update engine execution	Write			
ProvisionProduct	Grants permission to provision a product with a specified provisioning artifact and launch parameters	Write	Product*		
PutConfiguration	Grants permission to assign AppRegistry configurations	Write			
PutResourcePolicy [permission only]	Grants permission to add a resource-based policy for the specified resource	Write	Application		
			AttributeGroup		
RejectPortfolioShare	Grants permission to reject a portfolio that has been shared with you that you previously accepted	Write	Portfolio*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ScanProvisionedProducts	Grants permission to list all the provisioned products in your account	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
SearchProducts	Grants permission to list the products available to you as an end-user	List			
SearchProductsAsAdmin	Grants permission to list all the products in your account or all the products associated with a given portfolio	List			
SearchProvisionedProducts	Grants permission to list all the provisioned products in your account	List		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SyncResource	Grants permission to sync a resource with its current state in AppRegistry	Write			cloudformation:UpdateStack
TagResource	Grants permission to tag a service catalog appregistry resource	Tagging	Application		
			AttributeGroup		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateProvisionedProduct	Grants permission to terminate an existing provisioned product	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UntagResource	Grants permission to remove a tag from a service catalog appregistry resource	Tagging	Application		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Attribute Group		
				aws:TagKeys	
UpdateApplication	Grants permission to update the attributes of an existing application	Write	Application*		iam:CreateServiceLinkedRole
UpdateAttributeGroup	Grants permission to update the attributes of an existing attribute group	Write	AttributeGroup*		
UpdateConstraint	Grants permission to update the metadata fields of an existing constraint	Write			
UpdatePortfolio	Grants permission to update the metadata fields and/or tags of an existing portfolio	Write	Portfolio*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdatePortfolioShare	Grants permission to enable or disable resource sharing for an existing portfolio share	Permissions management	Portfolio*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProduct	Grants permission to update the metadata fields and/or tags of an existing product	Write	Product*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateProvisionedProduct	Grants permission to update an existing provisioned product	Write		servicecatalog:accountLevel servicecatalog:roleLevel servicecatalog:userLevel	
UpdateProvisionedProductProperties	Grants permission to update the properties of an existing provisioned product	Write			
UpdateProvisioningArtifact	Grants permission to update the metadata fields of an existing provisioning artifact	Write	Product*		
UpdateServiceAction	Grants permission to update a self-service action	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTagOption	Grants permission to update the specified TagOption	Write			

Resource types defined by AWS Service Catalog

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:${Partition}:servicecatalog:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
AttributeGroup	`arn:${Partition}:servicecatalog:${Region}:${Account}:/attribute-groups/${AttributeGroupId}`	aws:ResourceTag/${TagKey}
Portfolio	`arn:${Partition}:catalog:${Region}:${Account}:portfolio/${PortfolioId}`	aws:ResourceTag/${TagKey}
Product	`arn:${Partition}:catalog:${Region}:${Account}:product/${ProductId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Service Catalog

AWS Service Catalog defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the

policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

> **Note**
>
> For example policies that show how these condition keys can be used in an IAM policy, see Example Access Policies for Provisioned Product Management in the *Service Catalog Administrator Guide*.

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
servicecatalog:Resource	Filters access by controlling what value can be specified as the Resource parameter in an AppRegistry associate resource API	String
servicecatalog:ResourceType	Filters access by controlling what value can be specified as the ResourceType parameter in an AppRegistry associate resource API	String
servicecatalog:accountLevel	Filters access by user to see and perform actions on resources created by anyone in the account	String
servicecatalog:roleLevel	Filters access by user to see and perform actions on resources created either by them or by anyone federating into the same role as them	String

Condition keys	Description	Type
servicecatalog:userLevel	Filters access by user to see and perform actions on only resources that they created	String

Actions, resources, and condition keys for AWS service providing managed private networks

AWS service providing managed private networks (service prefix: `private-networks`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS service providing managed private networks
- Resource types defined by AWS service providing managed private networks
- Condition keys for AWS service providing managed private networks

Actions defined by AWS service providing managed private networks

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcknowledgeOrderReceipt	Grants permission to acknowledge that an order has been received	Write	order*		
ActivateDeviceIdentifier	Grants permission to activate a device identifier	Write	device-identifier*		
				aws:ResourceTag/${TagKey}	
ActivateNetworkSite	Grants permission to activate a network site	Write	network-site*		
			order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
ConfigureAccessPoint	Grants permission to configure an access point	Write	network-resource*		
CreateNetwork	Grants permission to create a network	Write	network*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateNetworkSite	Grants permission to create a network site	Write	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeactivateDeviceIdentifier	Grants permission to deactivate a device identifier	Write	device-identifier*		
DeleteNetwork	Grants permission to delete a network	Write	network*		
DeleteNetworkSite	Grants permission to delete a network site	Write	network-site*		
GetDeviceIdentifier	Grants permission to get a device identifier	Read	device-identifier*		
				aws:ResourceTag/${TagKey}	
GetNetwork	Grants permission to get a network	Read	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetNetworkResource	Grants permission to get a network resource	Read	network-resource*		
				aws:ResourceTag/${TagKey}	
GetNetworkSite	Grants permission to get a network site	Read	network-site*		
				aws:ResourceTag/${TagKey}	
GetOrder	Grants permission to get a network order	Read	order*		
				aws:ResourceTag/${TagKey}	
ListDeviceIdentifiers	Grants permission to list device identifiers	List	network*		
ListNetworkResources	Grants permission to list network resources	List	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNetworkSites	Grants permission to list network sites	List	network*		
ListNetworks	Grants permission to list networks	List			
ListOrders	Grants permission to list network orders	List	network*		
ListTagsForResource	Grants permission to return a list of tags for a resource	List			
Ping	Grants permission to check the health of the service	Read			
StartNetworkResourceUpdate	Grants permission to start an update on the specified network resource	Write	network-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to adds tags to the specified resource	Tagging	device-identifier		
			network		
			network-resource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-site		
			order		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to removes tags from the specified resource	Tagging	device-identifier		
			network		
			network-resource		
			network-site		
			order		
				aws:TagKeys	
UpdateNetworkSite	Grants permission to update a network site	Write	network-site*		
UpdateNetworkSitePlan	Grants permission to update a plan at a network site	Write	network-site*		

Resource types defined by AWS service providing managed private networks

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
network	`arn:${Partition}:private-networks:${Region}:${Account}:network/${NetworkName}`	aws:ResourceTag/${TagKey}
network-site	`arn:${Partition}:private-networks:${Region}:${Account}:network-site/${NetworkName}/${NetworkSiteName}`	aws:ResourceTag/${TagKey}
network-resource	`arn:${Partition}:private-networks:${Region}:${Account}:network-resource/${NetworkName}/${ResourceId}`	aws:ResourceTag/${TagKey}
order	`arn:${Partition}:private-networks:${Region}:${Account}:order/${NetworkName}/${OrderId}`	aws:ResourceTag/${TagKey}
device-identifier	`arn:${Partition}:private-networks:${Region}:${Account}:device-identifier/${NetworkName}/${DeviceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS service providing managed private networks

AWS service providing managed private networks defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by checking the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by checking tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by presence of tag keys in the request	ArrayOfString

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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateServiceQuotaTemplate	Grants permission to associate the Service Quotas template with your organization	Write			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
CreateSupportCase	Grants permission to submit a request to create a support case for an existing quota increase request	Write			
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 AWS default value	Read			
GetAssociationForS	Grants permission to retrieve the ServiceQuotaTempla	Read			organizations:Desc

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
erviceQuotaTemplate	teAssociationStatus value, which tells you if the Service Quotas template is associated with an organization				ribeOrganization
GetAutoManagementConfiguration	Grants permission to retrieve the automatic management of Service Quotas configuration, including notification settings, opt-in type, and excluded quotas	Read			
GetQuotaUtilizationReport	Grants permission to view the generated report	Read			
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	quota		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
				servicequotas:service	
GetServiceQuotaIncreaseRequestFromTemplate	Grants permission to retrieve the details for a service quota increase request from the service quota template	Read	quota		organizations:DescribeOrganization
				servicequotas:service	
ListAWSDefaultServiceQuotas	Grants permission to list all default service quotas for the specified AWS 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	quota		
				servicequotas:service	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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 AWS 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	
StartAutoManagement	Grants permission to enable automatic management of Service Quotas for an AWS account, including notification preferences and excluded quotas configurations	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartQuotaUtilizationReport	Grants permission to query quota utilization and create a report for your account	Read			
StopAutoManagement	Grants permission to stop automatic management of Service Quotas for an AWS account and remove all associated configurations	Write			
TagResource	Grants permission to associate a set of tags with an existing SQ resource	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
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	
UpdateAutoManagement	Grants permission to update the automatic management of Service Quotas configuration, including notification preferences and excluded quotas	Write			

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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
servicequotas:service	Filters access by the specified AWS service	String

Actions, resources, and condition keys for Amazon SES

Amazon SES (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by Amazon SES

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CloneReceiptRuleSet	Grants permission to create a receipt rule set by cloning an existing one	Write		ses:ApiVersion	
CreateConfigurationSet	Grants permission to create a new configuration set	Write		ses:ApiVersion	
CreateConfiguratio	Grants permission to create a configuration set event destination	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
nSetEvent Destination					
CreateConfiguratio nSetTrack ingOptions	Grants permission to creates an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion	
CreateCus tomVerifi cationEma ilTemplate	Grants permission to create a new custom verification email template	Write		ses:ApiVersion	
CreateRec eiptFilter	Grants permission to create a new IP address filter	Write		ses:ApiVersion	
CreateRec eiptRule	Grants permission to create a receipt rule	Write		ses:ApiVersion	
CreateRec eiptRuleSet	Grants permission to create an empty receipt rule set	Write		ses:ApiVersion	
CreateTem plate	Grants permission to creates an email template	Write		ses:ApiVersion	
DeleteCon figurationSet	Grants permission to delete an existing configuration set	Write		ses:ApiVersion	
DeleteConfiguratio nSetEvent Destination	Grants permission to delete an event destination	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConfigurationSetTrackingOptions	Grants permission to delete an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion	
DeleteCustomVerificationEmailTemplate	Grants permission to delete an existing custom verification email template	Write		ses:ApiVersion	
DeleteIdentity	Grants permission to delete the specified identity	Write		ses:ApiVersion	
DeleteIdentityPolicy	Grants permission to delete the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management		ses:ApiVersion	
DeleteReceiptFilter	Grants permission to delete the specified IP address filter	Write		ses:ApiVersion	
DeleteReceiptRule	Grants permission to delete the specified receipt rule	Write		ses:ApiVersion	
DeleteReceiptRuleSet	Grants permission to delete the specified receipt rule set and all of the receipt rules it contains	Write		ses:ApiVersion	
DeleteTemplate	Grants permission to delete an email template	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedEmailAddress	Grants permission to delete the specified email address from the list of verified addresses	Write		ses:ApiVersion	
DescribeActiveReceiptRuleSet	Grants permission to return the metadata and receipt rules for the receipt rule set that is currently active	Read		ses:ApiVersion	
DescribeConfigurationSet	Grants permission to return the details of the specified configuration set	Read		ses:ApiVersion	
DescribeReceiptRule	Grants permission to return the details of the specified receipt rule	Read		ses:ApiVersion	
DescribeReceiptRuleSet	Grants permission to return the details of the specified receipt rule set	Read		ses:ApiVersion	
GetAccountSendingEnabled	Grants permission to return the email sending status of your account	Read		ses:ApiVersion	
GetCustomVerificationEmailTemplate	Grants permission to return the custom email verification template for the template name you specify	Read		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdentityDkimAttributes	Grants permission to return the current status of Easy DKIM signing for an entity	Read		ses:ApiVersion	
GetIdentityMailFromDomainAttributes	Grants permission to return the custom MAIL FROM attributes for a list of identities (email addresses and/or domains)	Read		ses:ApiVersion	
GetIdentityNotificationAttributes	Grants permission to return a structure describing identity notification attributes for a list of verified identities (email addresses and/or domains),	Read		ses:ApiVersion	
GetIdentityPolicies	Grants permission to return the requested sending authorization policies for the given identity (an email address or a domain)	Read		ses:ApiVersion	
GetIdentityVerificationAttributes	Grants permission to return the verification status and (for domain identities) the verification token for a list of identities	Read		ses:ApiVersion	
GetSendQuota	Grants permission to return the user's current sending limits	Read		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSendStatistics	Grants permission to returns the user's sending statistics	Read		ses:ApiVersion	
GetTemplate	Grants permission to return the template object, which includes the subject line, HTML par, and text part for the template you specify	Read		ses:ApiVersion	
ListConfigurationSets	Grants permission to list all of the configuration sets for your account	List		ses:ApiVersion	
ListCustomVerificationEmailTemplates	Grants permission to list all of the existing custom verification email templates for your account	List		ses:ApiVersion	
ListIdentities	Grants permission to list the email identities for your account	List		ses:ApiVersion	
ListIdentityPolicies	Grants permission to list all of the email templates for your account	List		ses:ApiVersion	
ListReceiptFilters	Grants permission to list the IP address filters associated with your account	Read		ses:ApiVersion	
ListReceiptRuleSets	Grants permission to list the receipt rule sets that exist under your account	Read		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTemplates	Grants permission to list the email templates present in your account	List		ses:ApiVersion	
ListVerifiedEmailAddresses	Grants permission to list all of the email addresses that have been verified in your account	Read		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Grants permission to add or update the delivery options for a configuration set	Write		ses:ApiVersion	
PutIdentityPolicy	Grants permission to add or update a sending authorization policy for the specified identity (an email address or a domain)	Permissions management		ses:ApiVersion	
ReorderReceiptRuleSet	Grants permission to reorder the receipt rules within a receipt rule set	Write		ses:ApiVersion	
SendBounce	Grants permission to generate and send a bounce message to the sender of an email you received through Amazon SES	Write	identity*		
				ses:ApiVersion ses:FromAddress	
SendBulkTemplatedEmail	Grants permission to compose an email message to multiple destinations	Write	identity*		
			template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configuration-set		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendCustomVerificationEmail	Grants permission to add an email address to the list of identities and attempts to verify it for your account	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	Grants permission to send an email message	Write	identity*		
			configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	Grants permission to send an email message, with header and content specified by the client	Write	identity* configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	Grants permission to compose an email message using an email template	Write	identity*		
			template*		
			configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	Grants permission to set the specified receipt rule set as the active receipt rule set	Write		ses:ApiVersion	
SetIdentityDkimEnabled	Grants permission to enable or disable Easy DKIM signing of email sent from an identity	Write		ses:ApiVersion	
SetIdentityFeedbackForwardingEnabled	Grants permission to enable or disable whether Amazon SES forwards bounce and complaint notifications for an identity (an email address or a domain)	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetIdentityHeadersInNotificationsEnabled	Grants permission to set whether Amazon SES includes the original email headers in the Amazon Simple Notification Service (Amazon SNS) notifications of a specified type for a given identity (an email address or a domain)	Write		ses:ApiVersion	
SetIdentityMailFromDomain	Grants permission to enable or disable the custom MAIL FROM domain setup for a verified identity	Write		ses:ApiVersion	
SetIdentityNotificationTopic	Grants permission to set an Amazon Simple Notification Service (Amazon SNS) topic to use when delivering notifications for a verified identity	Write		ses:ApiVersion	
SetReceiptRulePosition	Grants permission to set the position of the specified receipt rule in the receipt rule set	Write		ses:ApiVersion	
TestRenderTemplate	Grants permission to create a preview of the MIME content of an email when provided with a template and a set of replacement data	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountSendingEnabled	Grants permission to enable or disable email sending for your account	Write		ses:ApiVersion	
UpdateConfigurationSetEventDestination	Grants permission to update the event destination of a configuration set	Write		ses:ApiVersion	
UpdateConfigurationSetReputationMetricsEnabled	Grants permission to enable or disable the publishing of reputation metrics for emails sent using a specific configuration set	Write		ses:ApiVersion	
UpdateConfigurationSetSendingEnabled	Grants permission to enable or disable email sending for messages sent using a specific configuration set	Write		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	Grants permission to modify an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	Grants permission to update an existing custom verification email template	Write		ses:ApiVersion	
UpdateReceiptRule	Grants permission to update a receipt rule	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTemplate	Grants permission to update an email template	Write		ses:ApiVersion	
VerifyDomainDkim	Grants permission to return a set of DKIM tokens for a domain	Write		ses:ApiVersion	
VerifyDomainIdentity	Grants permission to verify a domain	Write		ses:ApiVersion	
VerifyEmailAddress	Grants permission to verify an email address	Write		ses:ApiVersion	
VerifyEmailIdentity	Grants permission to verify an email identity	Write		ses:ApiVersion	

Resource types defined by Amazon SES

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	

Resource types	ARN	Condition keys
custom-verification-email-template	arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}	
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	

Condition keys for Amazon SES

Amazon SES defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
ses:ApiVersion	Filters actions based on the SES API version	String
ses:FeedbackAddress	Filters actions based on the "Return-Path" address, which specifies where bounces and complaints are sent by email feedback forwarding	String
ses:FromAddress	Filters actions based on the "From" address of a message	String
ses:FromDisplayName	Filters actions based on the "From" address that is used as the display name of a message	String

Condition keys	Description	Type
ses:Recipients	Filters actions based on the recipient addresses of a message, which include the "To", "CC", and "BCC" addresses	ArrayOfString

Actions, resources, and condition keys for AWS Shield

AWS Shield (service prefix: `shield`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Shield

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate DRTLogBucket	Grants permission to authorize the DDoS Response team to access the specified Amazon S3 bucket containing your flow logs	Write			s3:GetBucketPolicy s3:PutBucketPolicy
Associate DRTRole	Grants permission to authorize the DDoS Response team using the specified role, to access your AWS account to assist with DDoS attack mitigation during potential attacks	Write			iam:GetRole iam:ListAttachedRolePolicies iam:PassRole
Associate HealthCheck	Grants permission to add health-based detection to the Shield Advanced protection for a resource	Write	protection*		route53:GetHealthCheck
				aws:ResourceTag/${TagKey}	
Associate ProactiveEngagementDetails	Grants permission to initialize proactive engagement and set the list of contacts for the DDoS Response Team (DRT) to use	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProtection	Grants permission to activate DDoS protection service for a given resource ARN	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProtectionGroup	Grants permission to create a grouping of protected resources so they can be handled as a collective	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Grants permission to activate subscription	Write			
DeleteProtection	Grants permission to delete an existing protection	Write	protection*		
				aws:ResourceTag/${TagKey}	
DeleteProtectionGroup	Grants permission to remove the specified protection group	Write	protection-group*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubscription	Grants permission to deactivate subscription	Write			
DescribeAttack	Grants permission to get attack details	Read	attack*		
DescribeAttackContributors [permission only]	Grants permission to get detailed information about the contributors to a specific DDoS attack	Read	attack* protection-group		
DescribeAttackStatistics	Grants permission to describe information about the number and type of attacks AWS Shield has detected in the last year	Read			
DescribeDRTAccess	Grants permission to describe the current role and list of Amazon S3 log buckets used by the DDoS Response team to access your AWS account while assisting with attack mitigation	Read			
DescribeEmergencyContactSettings	Grants permission to list the email addresses that the DRT can use to contact you during a suspected attack	Read			
DescribeProtection	Grants permission to get protection details	Read	protection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DescribeProtectionGroup	Grants permission to describe the specification for the specified protection group	Read	protection-group*		
				aws:ResourceTag/${TagKey}	
DescribeSubscription	Grants permission to get subscription details, such as start time	Read			
DisableApplicationLayerAutomaticResponse	Grants permission to disable application layer automatic response for Shield Advanced protection for a resource	Write			
DisableProactiveEngagement	Grants permission to remove authorization from the DDoS Response Team (DRT) to notify contacts about escalations	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateDRTLogBucket	Grants permission to remove the DDoS Response team's access to the specified Amazon S3 bucket containing your flow logs	Write			s3:DeleteBucketPolicy s3:GetBucketPolicy s3:PutBucketPolicy
DisassociateDRTRole	Grants permission to remove the DDoS Response team's access to your AWS account	Write			
DisassociateHealthCheck	Grants permission to remove health-based detection from the Shield Advanced protection for a resource	Write	protection*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableApplicationLayerAutomaticResponse	Grants permission to enable application layer automatic response for Shield Advanced protection for a resource	Write			apprunner:DescribeWebAclForService cloudfront:GetDistribution cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl iam:CreateServiceLinkedRole iam:GetRole wafv2:GetWebACL wafv2:GetWebACLForResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableProactiveEngagement	Grants permission to authorize the DDoS Response Team (DRT) to use email and phone to notify contacts about escalations	Write			
GetGlobalThreatData [permission only]	Grants permission to retrieve global threat intelligence data and trends from AWS Shield's threat monitoring systems	Read			
GetSubscriptionState	Grants permission to get subscription state	Read			
ListAttacks	Grants permission to list all existing attacks	List			
ListMitigations [permission only]	Grants permission to retrieve a list of mitigation actions that have been applied during DDoS attacks	List	attack*		
ListProtectionGroups	Grants permission to retrieve the protection groups for the account	List			
ListProtections	Grants permission to list all existing protections	List			
ListResourcesInProtectionGroup	Grants permission to retrieve the resources that are included in the protection group	List	protection-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to get information about AWS tags for a specified Amazon Resource Name (ARN) in AWS Shield	Read	protection		
			protection-group		
TagResource	Grants permission to add or updates tags for a resource in AWS Shield	Tagging	protection		
			protection-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource in AWS Shield	Tagging	protection		
			protection-group		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplicationLayerAutomaticResponse	Grants permission to update application layer automatic response for Shield Advanced protection for a resource	Write			apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL wafv2:GetWebACLForResource
UpdateEmergencyContactSettings	Grants permission to update the details of the list of email addresses that the DRT can use to contact you during a suspected attack	Write			
UpdateProtectionGroup	Grants permission to update an existing protection group	Write	protection-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateSubscription	Grants permission to update the details of an existing subscription	Write			

Resource types defined by AWS Shield

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
attack	`arn:${Partition}:shield::${Account}:attack/${Id}`	
protection	`arn:${Partition}:shield::${Account}:protection/${Id}`	aws:ResourceTag/${TagKey}
protection-group	`arn:${Partition}:shield::${Account}:protection-group/${Id}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Shield

AWS Shield defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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 AWS Shield network security director

AWS Shield network security director (service prefix: `network-security-director`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Shield network security director

- Resource types defined by AWS Shield network security director
- Condition keys for AWS Shield network security director

Actions defined by AWS Shield network security director

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFinding	Grants permission to get a finding	Read			
GetResource	Grants permission to get a resource	Read			
ListAccountSummaries	Grants permission to list account summaries for an account	List			
ListFindings	Grants permission to list findings	List			
ListInsights	Grants permission to list insights about the latest network security scan	List			
ListRemediations	Grants permission to list remediations for a finding	List			
ListResources	Grants permission to list resources	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFinding	Grants permission to update the status of a finding	Write			

Resource types defined by AWS Shield network security director

AWS Shield network security director does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Shield network security director, specify `"Resource": "*"` in your policy.

Condition keys for AWS Shield network security director

Network Security Director has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Signer

AWS 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 AWS Signer
- Resource types defined by AWS Signer
- Condition keys for AWS Signer

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSigningProfile	Grants permission to return information about a specific Signing Profile	Read	signing-profile*		
				signer:ProfileVersion	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveProfilePermission	Grants permission to remove cross-account permissions from a Signing Profile	Permissions management	signing-profile*		
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add one or more tags to a Signing Profile	Tagging	signing-profile*		
				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 AWS 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 AWS Signer

AWS 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 AWS 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 AWS Signin

AWS Signin (service prefix: `signin`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Signin

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeOAuth2Access	Grants permission to authenticate through a browser and obtain an OAuth 2.0 authorization code for credential exchange	Read	oauth2-public-client-localhost*		
			oauth2-public-client-remote*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOAuth2Token	Grants permission to exchange an authorization code for OAuth 2.0 access token and refresh token that can be used to access AWS services from developer tools and applications	Read	oauth2-public-client-localhost*		
			oauth2-public-client-remote*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrustedIdentityPropagationApplicationForConsole	Grants permission to create an Identity Center application that represents the AWS Management Console on an Identity Center organization instance	Write			sso:CreateApplication sso:GetSharedSsoConfiguration sso:ListApplications sso:PutApplicationAccessScope sso:PutApplicationAssignmentConfiguration sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrustedIdentityPropagationApplicationsForConsole	Grants permission to list all Identity Center applications that represent the AWS Management Console	List			sso:GetSharedSsoConfiguration sso:ListApplications

Resource types defined by AWS Signin

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
oauth2-public-client-localhost	`arn:${Partition}:signin:${Region}:${Account}:oauth2/public-client/localhost`	
oauth2-public-client-remote	`arn:${Partition}:signin:${Region}:${Account}:oauth2/public-client/remote`	

Condition keys for AWS Signin

Signin has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Simple Email Service - Mail Manager

Amazon Simple Email Service - Mail Manager (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Simple Email Service - Mail Manager
- Resource types defined by Amazon Simple Email Service - Mail Manager
- Condition keys for Amazon Simple Email Service - Mail Manager

Actions defined by Amazon Simple Email Service - Mail Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for Mail Manager resources	Permissions management	mailmanager-ingress-point		
			mailmanager-rule-set		
CreateAddonInstance	Grants permission to create an addon instance	Write		aws:RequestTag/${TagKey} aws:TagKeys ses:AddonSubscriptionArn	
CreateAddonSubscription	Grants permission to create an addon subscription	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAddressList	Grants permission to create an address list	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateAddressListImportJob	Grants permission to create an import job on an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
CreateArchive	Grants permission to create an archive	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngressPoint	Grants permission to create an ingress point	Write		aws:RequestTag/${TagKey} aws:TagKeys ses:MailManagerRuleSetArn ses:MailManagerTrafficPolicyArn	ec2:DescribeVpcEndpoints iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRelay	Grants permission to create a SMTP relay	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleSet	Grants permission to create a rule set	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrafficPolicy	Grants permission to create a traffic policy	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddonInstance	Grants permission to delete an addon instance	Write	addon-instance*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAddonSubscription	Grants permission to delete an addon subscription	Write	addon-subscription*		
				aws:RequestTag/${TagKey}	
DeleteAddressList	Grants permission to delete an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
DeleteArchive	Grants permission to delete an archive	Write	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
DeleteIngressPoint	Grants permission to delete an ingress point	Write	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRelay	Grants permission to delete a SMTP relay	Write	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
DeleteRuleSet	Grants permission to delete a rule set	Write	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
DeleteTrafficPolicy	Grants permission to delete a traffic point	Write	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	
DeregisterMemberFromAddressList	Grants permission to remove a member from an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAddonInstance	Grants permission to get information about an addon instance	Read	addon-instance*		
				aws:RequestTag/${TagKey}	
GetAddonSubscription	Grants permission to get information about an addon subscription	Read	addon-subscription*		
				aws:RequestTag/${TagKey}	
GetAddressList	Grants permission to get information about an address list	Read	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddressListImportJob	Grants permission to get information about an import job on an address list	Read	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetArchive	Grants permission to get information about an archive	Read	mailmanager-archive*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
GetArchiveExport	Grants permission to get information about an archive export	Read	mailmanager-archive*		
GetArchiveMessage	Grants permission to retrieve archived message	Read	mailmanager-archive*		
GetArchiveMessageContent	Grants permission to retrieve archived message content	Read	mailmanager-archive*		
GetArchiveSearch	Grants permission to get information about a search	Read	mailmanager-archive*		
GetArchiveSearchResults	Grants permission to get information about search results	Read	mailmanager-archive*		
GetIngressPoint	Grants permission to get information about an ingress point	Read	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMemberOfAddressList	Grants permission to get information about a member in an address list	Read	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetRelay	Grants permission to get information about a SMTP relay	Read	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
GetRuleSet	Grants permission to get information about a rule set	Read	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
GetTrafficPolicy	Grants permission to get information about a traffic policy	Read	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAddonInstances	Grants permission to list all of the addon instances associated with your account	List			
ListAddonSubscriptions	Grants permission to list all of the addon subscriptions associated with your account	List			
ListAddressListImportJobs	Grants permission to list all of the import jobs associated with an address list	List	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListAddressLists	Grants permission to list all of the address lists associated with your account	List			
ListArchiveExports	Grants permission to list all of the archive exports associated with your account	List			
ListArchiveSearches	Grants permission to list all of the archive searches associated with your account	List			
ListArchives	Grants permission to list all of the archives associated with your account	List			
ListIngressPoints	Grants permission to list all of the ingress points associated with your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMembersOfAddressList	Grants permission to list all of the members associated with an address list	List	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListRelays	Grants permission to list all of the SMTP relays associated with your account	List			
ListRuleSets	Grants permission to list all of the rule sets associated with your account	List			
ListTagsForResource	Grants permission to list all of the tags associated with the resource	Read	addon-instance		
			addon-subscription		
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
ListTrafficPolicies	Grants permission to list all of the traffic policies associated with your account	List			
RegisterMemberToAddressList	Grants permission to add a member to an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartAddressListImportJob	Grants permission to start an import job on an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartArchiveExport	Grants permission to start an archive export	Write	mailmanager-archive*		
StartArchiveSearch	Grants permission to start an archive search	Write	mailmanager-archive*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopAddressListImportJob	Grants permission to stop an ongoing import job on an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StopArchiveExport	Grants permission to stop archive export	Write	mailmanager-archive*		
StopArchiveSearch	Grants permission to stop archive search	Write	mailmanager-archive*		
TagResource	Grants permission to add one or more tags (keys and values) to a specified resource	Tagging	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		
			mailmanager-ingress-point		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys	
UpdateArchive	Grants permission to update an archive	Write	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
UpdateIngressPoint	Grants permission to update an ingress point	Write	mailmanager-ingress-point*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} ses:MailManagerTrafficPolicyArn ses:MailManagerRuleSetArn	
UpdateRelay	Grants permission to update a SMTP relay	Write	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
UpdateRuleSet	Grants permission to update a rule set	Write	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTrafficPolicy	Grants permission to update a traffic policy	Write	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

Resource types defined by Amazon Simple Email Service - Mail Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
addon-instance	`arn:${Partition}:ses:${Region}:${Account}:addon-instance/${AddonInstanceId}`	aws:ResourceTag/${TagKey}
addon-subscription	`arn:${Partition}:ses:${Region}:${Account}:addon-subscription/${AddonSubscriptionId}`	aws:ResourceTag/${TagKey}
mailmanager-archive	`arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
mailmanager-ingress-point	arn:${Partition}:ses:${Region}:${Account}:mailmanager-ingress-point/${IngressPointId}	aws:ResourceTag/${TagKey} ses:MailManagerIngressPointType
mailmanager-smtp-relay	arn:${Partition}:ses:${Region}:${Account}:mailmanager-smtp-relay/${RelayId}	aws:ResourceTag/${TagKey}
mailmanager-rule-set	arn:${Partition}:ses:${Region}:${Account}:mailmanager-rule-set/${RuleSetId}	aws:ResourceTag/${TagKey}
mailmanager-traffic-policy	arn:${Partition}:ses:${Region}:${Account}:mailmanager-traffic-policy/${TrafficPolicyId}	aws:ResourceTag/${TagKey}
mailmanager-address-list	arn:${Partition}:ses:${Region}:${Account}:mailmanager-address-list/${AddressListId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Simple Email Service - Mail Manager

Amazon Simple Email Service - Mail Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
ses:AddonSubscriptionArn	Filters access by SES Addon Subscription ARN	ARN
ses:MailManagerIngressPointType	Filters access by SES Mail Manager ingress point type, for example OPEN or AUTH	String
ses:MailManagerRuleSetArn	Filters access by SES Mail Manager rule set ARN	ARN
ses:MailManagerTrafficPolicyArn	Filters access by SES Mail Manager traffic policy ARN	ARN

Actions, resources, and condition keys for Amazon Simple Email Service v2

Amazon Simple Email Service v2 (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by Amazon Simple Email Service v2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetMetricData	Grants permission to get metric data on your activity	Read	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	Grants permission to cancel an export job	Write	export-job*		
				ses:ApiVersion ses:ExportSourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfigurationSet	Grants permission to create a new configuration set	Write	configuration-set*		
			dedicated-ip-pool		
			mailmanager-archive		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContact	Grants permission to create a contact	Write	contact-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContactList	Grants permission to create a contact list	Write	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomVerificationEmailTemplate	Grants permission to create a new custom verification email template	Write	custom-verification-email-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDedicatedIpPool	Grants permission to create a new pool of dedicated IP addresses	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Grants permission to create a new predictive inbox placement test	Write	identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Grants permission to start the process of verifying an email identity	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentityPolicy	Grants permission to create the specified sending authorization policy for the given identity	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEmailTemplate	Grants permission to create an email template	Write	template*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportJob	Grants permission to create an export job	Write		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	Grants permission to creates an import job for a data destination	Write		ses:ApiVersion	
CreateMultiRegionEndpoint	Grants permission to create a new multi-region endpoint	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTenant	Grants permission to create a new tenant	Write	tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateTenantResourceAssociation	Grants permission to associate a SES resource to a tenant	Write	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Grants permission to delete an event destination	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContact	Grants permission to delete a contact from a contact list	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	Grants permission to delete a contact list with all of its contacts	Write	contact-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	Grants permission to delete an existing custom verification email template	Write	custom-verification-email-template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Grants permission to delete a dedicated IP pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEmailIdentity	Grants permission to delete an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentityPolicy	Grants permission to delete the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	Grants permission to delete an email template	Write	template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteMultiRegionEndpoint	Grants permission to delete a multi-region endpoint	Write	multi-region-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteSuppressedDestination	Grants permission to remove an email address from the suppression list for your account	Write		ses:ApiVersion	
DeleteTenant	Grants permission to delete a tenant	Write	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteTenantResourceAssociation	Grants permission to remove an associated SES resource from a tenant	Write	configuration-set*		
			identity*		
			template*		
			tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Grants permission to get information about the email-sending status and capabilities for your account	Read		ses:ApiVersion	
GetBlacklistReports	Grants permission to retrieve a list of the deny lists on which your dedicated IP addresses or tracked domains appear	Read		ses:ApiVersion	
GetConfigurationSet	Grants permission to get information about an existing configuration set	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Grants permission to retrieve a list of event destinations that are associated with a configuration set	Read	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContact	Grants permission to return a contact from a contact list	Read	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	Grants permission to return contact list metadata	Read	contact-list*		
				ses:ApiVersion	
GetCustomVerificationEmailTemplate	Grants permission to return the custom email verification template for the template name you specify	Read	custom-verification-email-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Grants permission to get information about a dedicated IP address	Read		ses:ApiVersion	
GetDedicatedIpPool	Grants permission to get information about a dedicated IP pool	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIps	Grants permission to list the dedicated IP addresses a dedicated IP pool	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDeliverabilityDashboardOptions	Grants permission to get the status of the Deliverability dashboard	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Grants permission to retrieve the results of a predictive inbox placement test	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Grants permission to retrieve all the deliverability data for a specific campaign	Read		ses:ApiVersion	
GetDomainStatisticsReport	Grants permission to retrieve inbox placement and engagement rates for the domains that you use to send email	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEmailAddressInsights	Grants permission to get insights about email address	Read		ses:ApiVersion	iam:CreateServiceLinkedRole
GetEmailIdentity	Grants permission to get information about a specific identity	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	Grants permission to return the requested sending authorization policies for the given identity (an email address or a domain)	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailTemplate	Grants permission to return the template object, which includes the subject line, HTML part, and text part for the template you specify	Read	template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExportJob	Grants permission to get information about an export job	Read	export-job*		
				ses:ApiVersion ses:ExportSourceType	
GetImportJob	Grants permission to provide information about an import job	Read	import-job*		
				ses:ApiVersion	
GetMessageInsights	Grants permission to provide insights about a message	Read		ses:ApiVersion	
GetMultiRegionEndpoint	Grants permission to get information about a multi-region endpoint	Read	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetReputationEntity		Read	tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve information about a reputation entity's status			ses:ApiVersion aws:ResourceTag/${TagKey}	
GetSuppressedDestination	Grants permission to retrieve information about a specific email address that's on the suppression list for your account	Read		ses:ApiVersion	
GetTenant	Grants permission to get information about a tenant	Read	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Grants permission to list all of the configuration sets for your account	List		ses:ApiVersion	
ListContactLists	Grants permission to list all of the contact lists available for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContacts	Grants permission to list the contacts present in a specific contact list	List	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	Grants permission to list all of the existing custom verification email templates for your account	List		ses:ApiVersion	
ListDedicatedIpPools	Grants permission to list all of the dedicated IP pools for your account	List		ses:ApiVersion	
ListDeliverabilityTestReports	Grants permission to retrieve the list of the predictive inbox placement tests that you've performed, regardless of their statuses, for your account	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Grants permission to list deliverability data for campaigns that used a specific domain to send email during a specified time range	Read		ses:ApiVersion	
ListEmailIdentities	Grants permission to list the email identities for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEmailTemplates	Grants permission to list all of the email templates for your account	List		ses:ApiVersion	
ListExportJobs	Grants permission to list all the exports jobs for your account	List		ses:ApiVersion ses:ExportSourceType	
ListImportJobs	Grants permission to list all of the import jobs for your account	List		ses:ApiVersion	
ListMultiRegionEndpoints	Grants permission to list all of the multi-region endpoints for your account	List		ses:ApiVersion	
ListRecommendations	Grants permission to list recommendations for your account	Read	identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListReputationEntities	Grants permission to retrieve a list of reputation entities	List	tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListResourceTenants	Grants permission to list all the tenants associated to a SES resource	List	configuration-set*		
			identity*		
			template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	Grants permission to list email addresses that are on the suppression list for your account	Read		ses:ApiVersion	
ListTagsForResource	Grants permission to retrieve a list of the tags (keys and values) that are associated with a specific resource for your account	Read	configuration-set		
			contact-list		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		
				ses:ApiVersion	
ListTenantResources	Grants permission to list all the resources associated to a tenant	List	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListTenants	Grants permission to list all the tenants for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccountDedicatedIpWarmupAttributes	Grants permission to enable or disable the automatic warm-up feature for dedicated IP addresses	Write		ses:ApiVersion	
PutAccountDetails	Grants permission to update your account details	Write		ses:ApiVersion	
PutAccountSendingAttributes	Grants permission to enable or disable the ability to send email for your account	Write		ses:ApiVersion	
PutAccountSuppressionAttributes	Grants permission to change the settings for the account-level suppression list	Write		ses:ApiVersion	
PutAccountVdmAttributes	Grants permission to change the settings for VDM for your account	Write		ses:ApiVersion	
PutConfigurationSetArchivingOptions	Grants permission to associate a configuration set with a Mail Manager archive	Write	configuration-set*		
			mailmanager-archive		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurationSetDeliveryOptions	Grants permission to associate a configuration set with a dedicated IP pool	Write	configuration-set*		
			dedicated-ip-pool		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Grants permission to enable or disable collection of reputation metrics for emails that you send using a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	Grants permission to enable or disable email sending for messages that use a particular configuration set	Write	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSuppressionOptions	Grants permission to specify the account suppression list preferences for a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Grants permission to specify a custom domain to use for open and click tracking elements in email that you send for a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetVdmOptions	Grants permission to override account-level VDM settings for a particular configuration set	Write	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Grants permission to move a dedicated IP address to an existing dedicated IP pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	Grants permission to transition a dedicated IP pool from Standard to Managed	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Grants permission to put Dedicated IP warm up attributes	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDeliverabilityDashboardOption	Grants permission to enable or disable the Deliverability dashboard	Write		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	Grants permission to associate a configuration set with an email identity	Write	identity*		
			configuration-set		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimAttributes	Grants permission to enable or disable DKIM authentication for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEmailIdentityDkimSigningAttributes	Grants permission to configure or change the DKIM authentication settings for an email domain identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Grants permission to enable or disable feedback forwarding for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Grants permission to enable or disable the custom MAIL FROM domain configuration for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutSuppressedDestination	Grants permission to add an email address to the suppression list	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplicateEmailIdentityDkimSigningKey [permission only]	Grants permission to replicate email identity DKIM signing key	Permissions management	identity*		
				ses:ReplicaRegion	
SendBulkEmail	Grants permission to compose an email message to multiple destinations	Write	identity*		
			template*		
			configuration-set		
				ses:ApiVersion ses:MultiRegionEndpointId ses:TenantName	
SendCustomVerificationEmail	Grants permission to add an email address to the list of identities and attempts to verify it	Write	custom-verification-email-template*		
				ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendEmail	Grants permission to send an email message	Write	identity*		
			configuration-set		
			template		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients ses:MultiRegionEndpointId ses:TenantName	
TagResource	Grants permission to add one or more tags (keys and values) to a specified resource	Tagging	configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			contact-list		
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestRenderEmailTemplate	Grants permission to create a preview of the MIME content of an email when provided with a template and a set of replacement data	Write	template*		
				ses:ApiVersion	
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	configuration-set		
			contact-list		
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Grants permission to update the configuration of an event destination for a configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	Grants permission to update a contact's preferences for a list	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContactList	Grants permission to update contact list metadata	Write	contact-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	Grants permission to update an existing custom verification email template	Write	custom-verification-email-template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailIdentityPolicy	Grants permission to update the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	Grants permission to update an email template	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityCustomerManagedStatus	Grants permission to update the customer-managed sending status	Write	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityPolicy	Grants permission to assign a reputation policy	Write	reputation-policy*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Simple Email Service v2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
reputation-policy	`arn:${Partition}:ses:${Region}:aws:reputation-policy/${ReputationPolicyName}`	
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
contact-list	`arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}`	aws:ResourceTag/${TagKey}
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	aws:ResourceTag/${TagKey}
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
export-job	`arn:${Partition}:ses:${Region}:${Account}:export-job/${ExportJobId}`	

Resource types	ARN	Condition keys
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	aws:ResourceTag/${TagKey}
import-job	arn:${Partition}:ses:${Region}:${Account}:import-job/${ImportJobId}	
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	aws:ResourceTag/${TagKey}
multi-region-endpoint	arn:${Partition}:ses:${Region}:${Account}:multi-region-endpoint/${EndpointName}	
mailmanager-archive	arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}	aws:ResourceTag/${TagKey}
tenant	arn:${Partition}:ses:${Region}:${Account}:tenant/${TenantName}/${TenantId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Simple Email Service v2

Amazon Simple Email Service v2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
ses:ApiVersion	Filters access by the SES API version	String
ses:ExportSourceType	Filters access by the export source type	String
ses:FeedbackAddress	Filters access by the "Return-Path" address, which specifies where bounces and complaints are sent by email feedback forwarding	String
ses:FromAddress	Filters access by the "From" address of a message	String
ses:FromDisplayName	Filters access by the "From" address that is used as the display name of a message	String
ses:MultiRegionEndpointId	Filters access by the multi-region endpoint ID that is used to send email	String
ses:Recipients	Filters access by the recipient addresses of a message, which include the "To", "CC", and "BCC" addresses	ArrayOfString
ses:ReplicaRegion	Filters access by the replica regions for Replicating domain DKIM signing key	ArrayOfString
ses:TenantName	Filters access by the tenant name that is used to send email	String

Actions, resources, and condition keys for Amazon Simple Workflow Service

Amazon Simple Workflow Service (service prefix: `swf`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by Amazon Simple Workflow Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTimer [permission only]	Grants permission to cancel a previously started timer and record a TimerCanceled event in the history	Write	domain*		
CancelWorkflowExecution	Grants permission to close the workflow execution and record a WorkflowExecutionCanceled event in the history	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
CompleteWorkflowExecution [permission only]	Grants permission to close the workflow execution and record a WorkflowExecutionCompleted event in the history	Write	domain*		
ContinueAsNewWorkflowExecution [permission only]	Grants permission to close the workflow execution and start a new workflow execution of the same type using the same workflow ID and a unique run Id	Write	domain*		
CountClosedWorkflowExecutions	Grants permission to return the number of closed workflow executions within the given domain that meet the specified filtering criteria	Read	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CountOpenWorkflowExecutions	Grants permission to return the number of open workflow executions within the given domain that meet the specified filtering criteria	Read	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountPendingActivityTasks	Grants permission to return the estimated number of activity tasks in the specified task list	Read	domain*		
				swf:taskList.name	
CountPendingDecisionTasks	Grants permission to return the estimated number of decision tasks in the specified task list	Read	domain*		
				swf:taskList.name	
DeleteActivityType	Grants permission to delete the specified activity type	Write	domain*		
				swf:activityType.name swf:activityType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWorkflowType	Grants permission to delete the specified workflow type	Write	domain*		
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	Grants permission to deprecate the specified activity type	Write	domain*		
				swf:activityType.name swf:activityType.version	
DeprecateDomain	Grants permission to deprecate the specified domain	Write	domain*		
DeprecateWorkflowType	Grants permission to deprecate the specified workflow type	Write	domain*		
				swf:workflowType.name swf:workflowType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeActivityType	Grants permission to return information about the specified activity type	Read	domain*		
				swf:activityType.name swf:activityType.version	
DescribeDomain	Grants permission to return information about the specified domain, including its description and status	Read	domain*		
DescribeWorkflowExecution	Grants permission to return information about the specified workflow execution including its type and some statistics	Read	domain*		
DescribeWorkflowType	Grants permission to return information about the specified workflow type	Read	domain*		
				swf:workflowType.name swf:workflowType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
FailWorkflowExecution [permission only]	Grants permission to close the workflow execution and record a WorkflowExecutionFailed event in the history	Write	domain*		
GetWorkflowExecutionHistory	Grants permission to return the history of the specified workflow execution	Read	domain*		
ListActivityTypes	Grants permission to return information about all activities registered in the specified domain that match the specified name and registration status	List	domain*		
ListClosedWorkflowExecutions	Grants permission to return a list of closed workflow executions in the specified domain that meet the filtering criteria	List	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListDomains	Grants permission to return the list of domains registered in the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOpenWorkflowExecutions	Grants permission to return a list of open workflow executions in the specified domain that meet the filtering criteria	List	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	Grants permission to list tags for an AWS SWF resource	List	domain		
ListWorkflowTypes	Grants permission to return information about workflow types in the specified domain	List	domain*		
PollForActivityTask	Grants permission to workers to get an ActivityTask from the specified activity taskList	Write	domain*		
				swf:taskList.name	
PollForDecisionTask	Grants permission to deciders to get a DecisionTask from the specified decision taskList	Write	domain*		
				swf:taskList.name	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RecordActivityTaskHeartbeat	Grants permission to workers to report to the service that the ActivityTask represented by the specified taskToken is still making progress	Write	domain*		
RecordMarker [permission only]	Grants permission to record a MarkerRecorded event in the history	Write	domain*		
RegisterActivityType	Grants permission to register a new activity type along with its configuration settings in the specified domain	Write	domain*		
				swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	Grants permission to register a new domain	Write		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterWorkflowType	Grants permission to register a new workflow type and its configuration settings in the specified domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [permission only]	Grants permission to attempt to cancel a previously scheduled activity task	Write	domain*		
RequestCancelExternalWorkflowExecution [permission only]	Grants permission to request that a request be made to cancel the specified external workflow execution	Write	domain*		
RequestCancelWorkflowExecution	Grants permission to record a WorkflowExecutionCancelRequested event in the currently running workflow execution identified by the given domain, workflowId, and runId	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RespondActivityTaskCanceled	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken was successfully canceled	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RespondActivityTaskCompleted	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken completed successfully with a result (if provided)	Write	domain*		
				swf:activityType.name swf:activityType.version swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken has failed with reason (if specified)	Write	domain*		
RespondDecisionTaskCompleted	Grants permission to deciders to tell the service that the DecisionTask identified by the taskToken has successfully completed	Write	domain*		
ScheduleActivityTask [permission only]	Grants permission to schedule an activity task	Write	domain*		
SignalExternalWorkflowExecution [permission only]	Grants permission to request a signal to be delivered to the specified external workflow execution and records	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SignalWorkflowExecution	Grants permission to record a WorkflowExecutionSignaled event in the workflow execution history and create a decision task for the workflow execution identified by the given domain, workflowId and runId	Write	domain*		
StartChildWorkflowExecution [permission only]	Grants permission to request that a child workflow execution be started	Write	domain*		
StartTimer [permission only]	Grants permission to start a timer for a workflow execution	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartWorkflowExecution	Grants permission to start an execution of the workflow type in the specified domain using the provided workflowId and input data	Write	domain*	swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name swf:workflowType.name swf:workflowType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an AWS SWF resource	Tagging	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	Grants permission to record a WorkflowExecutionTerminated event and force closure of the workflow execution identified by the given domain, runId, and workflowId	Write	domain*		
UndeprecateActivityType	Grants permission to undeprecate a previously deprecated activity type	Write	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	Grants permission to undeprecate a previously deprecated domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UndeprecateWorkflowType	Grants permission to undeprecate a previously deprecated workflow type	Write	domain*		
				swf:workflowType.name swf:workflowType.version	
UntagResource	Grants permission to remove a tag from an AWS SWF resource	Tagging	domain		
				aws:TagKeys	

Resource types defined by Amazon Simple Workflow Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Simple Workflow Service

Amazon Simple Workflow Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag of the request	String
aws:ResourceTag/${TagKey}	Filters access by tag of the resource	String
aws:TagKeys	Filters access by tag of the key	ArrayOfString
swf:activityType.name	Filters access by the name of the activity type	String
swf:activityType.version	Filters access by the version of the activity type	String
swf:defaultTaskList.name	Filters access by the name of the default task list	String
swf:name	Filters access by the name of activities or workflows	String
swf:tagFilter.tag	Filters access by the value of tagFilter.tag	String
swf:tagList.member.0	Filters access by the specified tag	String
swf:tagList.member.1	Filters access by the specified tag	String

Condition keys	Description	Type
swf:tagList.member.2	Filters access by the specified tag	String
swf:tagList.member.3	Filters access by the specified tag	String
swf:tagList.member.4	Filters access by the specified tag	String
swf:taskList.name	Filters access by the name of the tasklist	String
swf:typeFilter.name	Filters access by the name of the type filter	String
swf:typeFilter.version	Filters access by the version of the type filter	String
swf:version	Filters access by the version of activities or workflows	String
swf:workflowType.name	Filters access by the name of the workflow type	String
swf:workflowType.version	Filters access by the version of the workflow type	String

Actions, resources, and condition keys for Amazon 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteAttributes	Grants permission to perform multiple DeleteAttributes operations in a single call, which reduces round trips and latencies	Write	domain*		
BatchPutAttributes	Grants permission to perform multiple PutAttribute operations in a single call, which reduces round trips and latencies	Write	domain*		
CreateDomain	Grants permission to create a new domain	Write	domain*		
DeleteAttributes	Grants permission to delete one or more attributes associated with the item	Write	domain*		
DeleteDomain	Grants permission to delete a domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DomainMetadata	Grants permission to return information about the domain, including when the domain was created, the number of items and attributes, and the size of attribute names and values	Read	domain*		
GetAttributes	Grants permission to return all of the attributes associated with the item	Read	domain*		
GetExport	Grants permission to return information for an existing domain export arn	Read	export*		
ListDomains	Grants permission to list all domains	List			
ListExports	Grants permission to list all exports that were created. The results are paginated and can be filtered by domain name	List	domain		
PutAttributes	Grants permission to create or replace attributes in an item	Write	domain*		
Select	Grants permission to execute a query against the items in a domain	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDomainExport	Grants permission to initiates the export of a SimpleDB domain to an S3 bucket	Write	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}`	
export	`arn:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}/export/${ExportUUID}`	

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 AWS global condition context keys.

Actions, resources, and condition keys for AWS SimSpace Weaver

AWS SimSpace Weaver (service prefix: `simspaceweaver`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS SimSpace Weaver

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshot	Grants permission to create a snapshot	Write	Simulation*		
DeleteApp	Grants permission to delete an app	Write	Simulation*		
DeleteSimulation	Grants permission to delete a simulation	Write	Simulation*		
DescribeApp	Grants permission to describe an app	Read	Simulation*		
DescribeSimulation	Grants permission to describe a simulation	Read	Simulation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApps	Grants permission to list apps	Read	Simulation*		
ListSimulations	Grants permission to list simulations	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read			
StartApp	Grants permission to start an app	Write	Simulation*		
StartClock	Grants permission to start a simulation clock	Write	Simulation*		
StartSimulation	Grants permission to start a simulation	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopApp	Grants permission to stop an app	Write	Simulation*		
StopClock	Grants permission to stop a simulation clock	Write	Simulation*		
StopSimulation	Grants permission to stop a simulation	Write	Simulation*		
TagResource	Grants permission to tag a resource	Tagging	Simulation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	Simulation*		
				aws:TagKeys	

Resource types defined by AWS SimSpace Weaver

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
Simulation	`arn:${Partition}:simspaceweaver:${Region}:${Account}:simulation/${SimulationName}`	aws:ResourceTag/${TagKey}

Condition keys for AWS SimSpace Weaver

AWS SimSpace Weaver defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Snow Device Management

AWS Snow Device Management (service prefix: `snow-device-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 AWS Snow Device Management

- Resource types defined by AWS Snow Device Management
- Condition keys for AWS Snow Device Management

Actions defined by AWS Snow Device Management

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTask	Grants permission to cancel tasks on remote devices	Write	task*		
CreateTask	Grants permission to create tasks on remote devices	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeDevice	Grants permission to describe a remotely-managed device	Read	managed-device*		
DescribeDeviceEc2Instances	Grants permission to describe a remotely-managed device's EC2 instances	Read	managed-device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeExecution	Grants permission to describe task executions	Read			
DescribeTask	Grants permission to describe a task	Read	task*		
ListDeviceResources	Grants permission to list a remotely-managed device's resources	List	managed-device*		
ListDevices	Grants permission to list remotely-managed devices	List			
ListExecutions	Grants permission to list task executions	List			
ListTagsForResource	Grants permission to list the tags for a resource (device or task)	Read		aws:RequestTag/${TagKey} aws:TagKeys	
ListTasks	Grants permission to list tasks	List			
TagResource	Grants permission to tag a resource	Tagging	managed-device		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	managed-device		
			task		
				aws:TagKeys	

Resource types defined by AWS Snow Device 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
managed-device	`arn:${Partition}:snow-device-management:${Region}:${Account}:managed-device/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
task	arn:${Partition}:snow-device-management:${Region}:${Account}:task/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Snow Device Management

AWS Snow Device Management defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
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 attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Snowball

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	allowing customers to add an upfront billing contract for a job				
CreateReturnShippingLabel	Grants permission to create a shipping label that will be used to return the Snow device to AWS	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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReturnShippingLabel	Grants permission to describe information on the shipping label of a Snow device that is being returned to AWS	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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account that would be supported for use on a Snow device	List			
ListJobs	Grants permission to list JobListEntry objects of the specified length	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
UpdateLongTermPricing	Grants permission to update a specific upfront billing contract for a job	Write			

Resource types defined by AWS Snowball

AWS Snowball does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Snowball, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPermission	Grants permission to add a statement to a topic's access control policy, granting access for the specified AWS accounts to the specified actions	Permissions management	topic*		
CheckIfPhoneNumberIsOptedOut	Grants permission to accept a phone number and indicate whether the phone holder has	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	opted out of receiving SMS messages from your account				
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 services, such as GCM and APNS	Write			
CreateSMSSandboxPhoneNumber	Grants permission to add a destination phone number and send a one-time password (OTP) to that phone number for an AWS account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DeleteSMSSandboxPhoneNumber	Grants permission to delete an AWS 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	Grants permission to verify a destination phone number with a one-time password (OTP) for an AWS 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 AWS 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

Condition keys	Description	Type
sns:Protocol	Filters access by the protocol value from a Subscribe request or a previously confirmed subscription	String

Actions, resources, and condition keys for AWS SQL Workbench

AWS 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 AWS SQL Workbench
- Resource types defined by AWS SQL Workbench
- Condition keys for AWS SQL Workbench

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateConnectionWithChart	Grants permission to associate connection to a chart	Write	chart*		
			connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
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 AWS 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 AWS SQL Workbench

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPermission	Grants permission to a queue for a specific principal	Permissions management	queue*		
CancelMessageMoveTask	Grants permission to cancel an in progress message move task	Write	queue*		
ChangeMessageVisibility	Grants permission to change the visibility timeout of a specified message in a queue to a new value	Write	queue*		
CreateQueue	Grants permission to create a new queue, or returns the URL of an existing one	Write	queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagQueue	Grants permission to remove tags from the specified SQS queue	Tagging	queue*		
				aws:TagKeys	

Resource types defined by Amazon SQS

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

> **Note**
>
> The ARN of the queue is used only in IAM permission policies. In API and CLI calls, you use the queue's URL instead.

Resource types	ARN	Condition keys
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon SQS

Amazon SQS defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Step Functions

AWS Step Functions (service prefix: `states`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Step Functions
- Resource types defined by AWS Step Functions
- Condition keys for AWS Step Functions

Actions defined by AWS Step Functions

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateActivity	Grants permission to create an activity	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	Grants permission to create a state machine	Write	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStateMachineAlias	Grants permission to create a state machine alias	Write	statemachine*		
				states:StateMachineQualifier	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeExecution	Grants permission to describe an execution	Read	execution*		
			express*		
DescribeMapRun	Grants permission to describe a map run	Read	maprun*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ListStateMachines	Grants permission to lists the existing state machines	List			
ListTagsForResource	Grants permission to list tags for an AWS Step Functions resource	List	activity		
			statemachine		
PublishStateMachineVersion	Grants permission to publish a state machine version	Write	statemachine*		
RedriveExecution	Grants permission to redrive an execution	Write	execution*		
RevealSecrets [permission only]	Grants permission to reveal sensitive data from an execution	Read			
SendTaskFailure	Grants permission to report that the task identified by the taskToken failed	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
StartExecution	Grants permission to start a state machine execution	Write	statemachine*		
				states:StateMachineQualifier	
StartSyncExecution	Grants permission to start a Synchronous Express state machine execution	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	Grants permission to stop an execution	Write	execution*		
TagResource	Grants permission to tag an AWS Step Functions resource	Tagging	activity		
			statemachine		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TestState	Grants permission to test a state machine definition	Write			states:RevealSecrets
UntagResource	Grants permission to remove a tag from an AWS Step Functions resource	Tagging	activity		
			statemachine		
				aws:TagKeys	
UpdateMapRun	Grants permission to update a map run	Write	maprun*		
UpdateStateMachine	Grants permission to update a state machine	Write	statemachine*		iam:PassRole states:PublishStateMachineVersion

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	Grants permission to update a state machine alias	Write	statemachine*		
				states:StateMachineQualifier	
ValidateStateMachineDefinition	Grants permission to validate a state machine definition	Read			

Resource types defined by AWS Step Functions

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
activity	arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}	aws:ResourceTag/${TagKey}
execution	arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}	aws:ResourceTag/${TagKey}
express	arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}:${ExecutionId}:${ExpressId}	
statemachine	arn:${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 AWS Step Functions

AWS Step Functions defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
states:HTTPEndpoint	Filters access by the endpoint that the HTTP Task state allows in the request	String
states:HTTPMethod	Filters access by the method that the HTTP Task state allows in the request	String
states:StateMachineQualifier	Filters access by the qualifier of a state machine ARN	ArrayOfString

Actions, resources, and condition keys for AWS Storage Gateway

AWS Storage Gateway (service prefix: `storagegateway`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Storage Gateway

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateGateway	Grants permission to activate the gateway you previously deployed on your host	Write		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	Grants permission to configure one or more gateway local disks as cache for a cached-volume gateway	Write	gateway*		
AddTagsToResource	Grants permission to add one or more tags to the specified resource	Tagging	cache-report		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
AddUploadBuffer	Grants permission to configure one or more gateway local disks as upload buffer for a specified gateway	Write	gateway*		
AddWorkingStorage	Grants permission to configure one or more gateway local disks as working storage for a gateway	Write	gateway*		
AssignTapePool		Write	tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to move a tape to the target pool specified		tapepool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate FileSystem	Grants permission to associate an Amazon FSx file system with the Amazon FSx file gateway	Write	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	Grants permission to connect a volume to an iSCSI connection and then attaches the volume to the specified gateway	Write	gateway* volume*		
BypassGovernanceRetention	Grants permission to allow the governance retention lock on a pool to be bypassed	Write	tapepool*		
CancelArchival	Grants permission to cancel archiving of a virtual tape to the virtual tape shelf (VTS) after the archiving process is initiated	Write	gateway* tape*		
CancelCacheReport	Grants permission to cancel a cache report	Write	cache-report*		
CancelRetrieval	Grants permission to cancel retrieval of a virtual tape from the virtual tape shelf (VTS) to a gateway after the retrieval process is initiated	Write	gateway* tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCachediSCSIVolume	Grants permission to create a cached volume on a specified cached gateway. This operation is supported only for the gateway-cached volume architecture	Write	gateway*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	Grants permission to create a NFS file share on an existing file gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	Grants permission to create a SMB file share on an existing file gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Grants permission to initiate a snapshot of a volume	Write	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	Grants permission to initiate a snapshot of a gateway from a volume recovery point	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	Grants permission to create a volume on a specified gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTapePool	Grants permission to create a tape pool	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	Grants permission to create a virtual tape by using your own barcode	Write	gateway* tapepool*	 aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	Grants permission to create one or more virtual tapes. You write data to the virtual tapes and then archive the tapes	Write	gateway* tapepool*	 aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAutomaticTapeCreationPolicy	Grants permission to delete the automatic tape creation policy configured on a gateway-VTL	Write	gateway*		
DeleteBandwidthRateLimit	Grants permission to delete the bandwidth rate limits of a gateway	Write	gateway*		
DeleteCacheReport	Grants permission to delete the metadata associated with a cache report	Write	cache-report*		
DeleteChapCredentials	Grants permission to delete Challenge-Handshake Authentication Protocol (CHAP) credentials for a specified iSCSI target and initiator pair	Write	target*		
DeleteFileShare	Grants permission to delete a file share from a file gateway	Write	share*		
DeleteGateway	Grants permission to delete a gateway	Write	gateway*		
DeleteSnapshotSchedule	Grants permission to delete a snapshot of a volume	Write	volume*		
DeleteTape	Grants permission to delete the specified virtual tape	Write	gateway* tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTapeArchive	Grants permission to delete the specified virtual tape from the virtual tape shelf (VTS)	Write			
DeleteTapePool	Grants permission to delete the specified tape pool	Write	tapepool*		
DeleteVolume	Grants permission to delete the specified gateway volume that you previously created using the CreateCachediSCSIVolume or CreateStorediSCSIVolume API	Write	volume*		
DescribeAvailabilityMonitorTest	Grants permission to get the information about the most recent high availability monitoring test that was performed on the gateway	Read	gateway*		
DescribeBandwidthRateLimit	Grants permission to get the bandwidth rate limits of a gateway	Read	gateway*		
DescribeBandwidthRateLimitSchedule	Grants permission to get the bandwidth rate limit schedule of a gateway	Read	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCache	Grants permission to get information about the cache of a gateway. This operation is supported only for the gateway-cached volume architecture	Read	gateway*		
DescribeCacheReport	Grants permission to get a description of a cache report	Read	cache-report*		
DescribeCachediSCSIVolumes	Grants permission to get a description of the gateway volumes specified in the request. This operation is supported only for the gateway-cached volume architecture	Read	volume*		
DescribeChapCredentials	Grants permission to get an array of Challenge-Handshake Authentication Protocol (CHAP) credentials information for a specified iSCSI target, one for each target-initiator pair	Read	target*		
DescribeFileSystemAssociations	Grants permission to get a description for one or more file system associations	Read	fs-association*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGatewayInformation	Grants permission to get metadata about a gateway such as its name, network interfaces, configured time zone, and the state (whether the gateway is running or not)	Read	gateway*		
DescribeMaintenanceStartTime	Grants permission to get your gateway's weekly maintenance start time including the day and time of the week	Read	gateway*		
DescribeNFSFileShares	Grants permission to get a description for one or more file shares from a file gateway	Read	share*		
DescribeSMBFileShares	Grants permission to get a description for one or more file shares from a file gateway	Read	share*		
DescribeSMBSettings	Grants permission to get a description of a Server Message Block (SMB) file share settings from a file gateway	Read	gateway*		
DescribeSnapshotSchedule	Grants permission to describe the snapshot schedule for the specified gateway volume	Read	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStorediSCSIVolumes	Grants permission to get the description of the gateway volumes specified in the request	Read	volume*		
DescribeTapeArchives	Grants permission to get a description of specified virtual tapes in the virtual tape shelf (VTS)	Read			
DescribeTapeRecoveryPoints	Grants permission to get a list of virtual tape recovery points that are available for the specified gateway-VTL	Read	gateway*		
DescribeTapes	Grants permission to get a description of the specified Amazon Resource Name (ARN) of virtual tapes	Read	gateway*		
DescribeUploadBuffer	Grants permission to get information about the upload buffer of a gateway	Read	gateway*		
DescribeVTLDevices	Grants permission to get a description of virtual tape library (VTL) devices for the specified gateway	Read	gateway*		
DescribeWorkingStorage	Grants permission to get information about the working storage of a gateway	Read	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachVolume	Grants permission to disconnect a volume from an iSCSI connection and then detaches the volume from the specified gateway	Write	volume*		
DisableGateway	Grants permission to disable a gateway when the gateway is no longer functioning	Write	gateway*		
DisassociateFileSystem	Grants permission to disassociate an Amazon FSx file system from an Amazon FSx file gateway	Write	fs-association*		
EvictFilesFailingUpload	Grants permission to clean a share's cache of file entries that are failing upload to Amazon S3	Write	share*		
JoinDomain	Grants permission to enable you to join an Active Directory Domain	Write	gateway*		
ListAutomaticTapeCreationPolicies	Grants permission to list the automatic tape creation policies configured on the specified gateway-VTL or all gateway-VTLs owned by your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCacheReports	Grants permission to get a list of the cache reports owned by your AWS account	List			
ListFileShares	Grants permission to get a list of the file shares for a specific file gateway, or the list of file shares owned by your AWS account	List			
ListFileSystemAssociations	Grants permission to get a list of the file system associations for the specified gateway	List			
ListGateways	Grants permission to list gateways owned by an AWS account in a region specified in the request. The returned list is ordered by gateway Amazon Resource Name (ARN)	List			
ListLocalDisks	Grants permission to get a list of the gateway's local disks	List	gateway*		
ListTagsForResource	Grants permission to get the tags that have been added to the specified resource	List	gateway		
			share		
			tape		
			volume		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTapePools	Grants permission to list tape pools owned by your AWS account	List			
ListTapes	Grants permission to list virtual tapes in your virtual tape library (VTL) and your virtual tape shelf (VTS)	List			
ListVolumeInitiators	Grants permission to list iSCSI initiators that are connected to a volume	List	volume*		
ListVolumeRecoveryPoints	Grants permission to list the recovery points for a specified gateway	List	gateway*		
ListVolumes	Grants permission to list the iSCSI stored volumes of a gateway	List			
NotifyWhenUploaded	Grants permission to send you a notification through CloudWatch Events when all files written to your NFS file share have been uploaded to Amazon S3	Write	share*		
RefreshCache	Grants permission to refresh the cache for the specified file share	Write	share*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveTagsFromResource	Grants permission to remove one or more tags from the specified resource	Tagging	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	
ResetCache	Grants permission to reset all cache disks that have encountered a error and makes the disks available for reconfiguration as cache storage	Write	gateway*		
RetrieveTapeArchive	Grants permission to retrieve an archived virtual tape from the virtual tape shelf (VTS) to a gateway-VTL	Write	gateway*		
			tape*		
RetrieveTapeRecoveryPoint	Grants permission to retrieve the recovery point for the specified virtual tape	Write	gateway*		
			tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLocalConsolePassword	Grants permission to set the password for your VM local console	Write	gateway*		
SetSMBGuestPassword	Grants permission to set the password for SMB Guest user	Write	gateway*		
ShutdownGateway	Grants permission to shut down a gateway	Write	gateway*		
StartAvailabilityMonitorTest	Grants permission to start a test that verifies that the specified gateway is configured for High Availability monitoring in your host environment	Write	gateway*		
StartCacheReport	Grants permission to start a cache report for an existing file share	Write	share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	Grants permission to start a gateway that you previously shut down	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAutomaticTapeCreationPolicy	Grants permission to update the automatic tape creation policy configured on a gateway-VTL	Write	gateway* tapepool*		
UpdateBandwidthRateLimit	Grants permission to update the bandwidth rate limits of a gateway	Write	gateway*		
UpdateBandwidthRateLimitSchedule	Grants permission to update the bandwidth rate limit schedule of a gateway	Write	gateway*		
UpdateChapCredentials	Grants permission to update the Challenge-Handshake Authentication Protocol (CHAP) credentials for a specified iSCSI target	Write	target*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFileSystemAssociation	Grants permission to update a file system association	Write	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	Grants permission to update a gateway's metadata, which includes the gateway's name and time zone	Write	gateway*		
UpdateGatewaySoftwareNow	Grants permission to update the gateway virtual machine (VM) software	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMaintenanceStartTime	Grants permission to update a gateway's weekly maintenance start time information, including day and time of the week. The maintenance time is the time in your gateway's time zone	Write	gateway*		
UpdateNFSFileShare	Grants permission to update a NFS file share	Write	share*		
UpdateSMBFileShare	Grants permission to update a SMB file share	Write	share*		
UpdateSMBFileShareVisibility	Grants permission to update whether the shares on a gateway are visible in a net view or browse list	Write	gateway*		
UpdateSMBLocalGroups	Grants permission to update the list of Active Directory users and groups that have special permissions for SMB file shares on the gateway	Write	gateway*		
UpdateSMBSecurityStrategy	Grants permission to update the SMB security strategy on a file gateway	Write	gateway*		
UpdateSnapshotSchedule	Grants permission to update a snapshot schedule configured for a gateway volume	Write	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	Grants permission to update the type of medium changer in a gateway-VTL	Write	device*		

Resource types defined by AWS Storage Gateway

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cache-report	`arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}/cache-report/${CacheReportId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}`	

Resource types	ARN	Condition keys
fs-association	arn:${Partition}:storagegateway:${Region}:${Account}:fs-association/${FsaId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
share	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}	aws:ResourceTag/${TagKey}
tape	arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}	aws:ResourceTag/${TagKey}
tapepool	arn:${Partition}:storagegateway:${Region}:${Account}:tapepool/${PoolId}	aws:ResourceTag/${TagKey}
target	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}	
volume	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Storage Gateway

AWS Storage Gateway defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Supply Chain

AWS Supply Chain (service prefix: `scn`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Supply Chain
- Resource types defined by AWS Supply Chain
- Condition keys for AWS Supply Chain

Actions defined by AWS Supply Chain

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignAdminPermissionsToUser	Grants permission to add AWS Supply Chain administrator permission to federated user	Write	instance*		
CreateBillOfMaterialsImportJob	Grants permission to create a BillOfMaterialsImportJob which will import a CSV file of BillOfMaterials records	Write	instance*		
CreateDataIntegrationFlow	Grants permission to create DataIntegrationFlow that can transform from multiple sources to one target	Write	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeDataset	Grants permission to create the data lake dataset	Write	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataLakeNamespace	Grants permission to create the data lake namespace	Write	instance*		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateInstance	Grants permission to create a new AWS Supply Chain instance	Write	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSSOApplication	Grants permission to create IAM Identity Center application for a AWS Supply Chain instance	Write	instance*		
DeleteDataIntegrationFlow	Grants permission to delete the DataIntegrationFlow	Write	data-integration-flow*		
DeleteDataLakeDataset	Grants permission to delete the data lake dataset	Write	dataset*		
DeleteDataLakeNamespace	Grants permission to delete the data lake namespace	Write	namespace*		
DeleteInstance	Grants permission to delete an AWS Supply Chain instance	Write	instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSSOApplication	Grants permission to delete IAM Identity Center application of the AWS Supply Chain instance	Write	instance*		
DescribeInstance	Grants permission to view details of an AWS Supply Chain instance	Read	instance*		
GetBillOfMaterialsImportJob	Grants permission to view status and details of a BillOfMaterialsImportJob	Read	bill-of-materials-import-job*		
GetDataIntegrationEvent	Grants permission to get a DataIntegrationEvent	Read	instance*		
GetDataIntegrationFlow	Grants permission to get the DataIntegrationFlow details	Read	data-integration-flow*		
GetDataIntegrationFlowExecution	Grants permission to get a particular execution of one specified DataIntegrationFlow	Read	data-integration-flow*		
GetDataLakeDataset	Grants permission to get the dataset details	Read	dataset*		
GetDataLakeNamespace	Grants permission to get the namespace details	Read	namespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstance	Grants permission to view details of an AWS Supply Chain instance	Read	instance*		
ListAdminUsers	Grants permission to list AWS Supply Chain administrators of an instance	List	instance*		
ListDataIntegrationEvents	Grants permission to list all DataIntegrationEvents under an instance	List	instance*		
ListDataIntegrationFlowExecutions	Grants permission to list all executions of one specified DataIntegrationFlow	List	data-integration-flow*		
ListDataIntegrationFlows	Grants permission to list all the DataIntegrationFlows in a paginated way	List	instance*		
ListDataLakeDatasets	Grants permission to list the data lake datasets under specific instance or namespace	List	instance*		
ListDataLakeNamespaces	Grants permission to list the data lake namespaces under specific instance	List	instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstances	Grants permission to view the AWS Supply Chain instances associated with an AWS account	List	instance*		
ListTagsForResource	Grants permission to list tags for an AWS Supply Chain resource	List	instance*		
RemoveAdminPermissionsForUser	Grants permission to remove AWS Supply Chain administrator permission from federated user	Write	instance*		
SendDataIntegrationEvent	Grants permission to create a DataIntegrationEvent which will ingest data in real-time	Write	instance*		
TagResource	Grants permission to tag an AWS Supply Chain resource	Tagging	instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tag from an AWS Supply Chain resource	Tagging	instance*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataIntegrationFlow	Grants permission to update the DataIntegrationFlow	Write	data-integration-flow*		
UpdateDataLakeDataset	Grants permission to update the data lake dataset	Write	dataset*		
UpdateDataLakeNamespace	Grants permission to update the data lake namespace	Write	namespace*		
UpdateInstance	Grants permission to update an AWS Supply Chain instance	Write	instance*		

Resource types defined by AWS Supply Chain

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:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey}
bill-of-materials-import-job	`arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/bill-of-materials-import-job/${JobId}`	

Resource types	ARN	Condition keys
data-integration-flow	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/data-integration-flows/${FlowName}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:scn:${Region}:${Account}:instance/${InstanceId}/namespaces/${Namespace}/datasets/${DatasetName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Supply Chain

AWS Supply Chain defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by using tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by using tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by using tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS Support

AWS Support (service prefix: `support`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Support

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

> **Note**
>
> Support provides the ability to access, modify and resolve cases, as well as use Trusted Advisor actions. When you use the Support API to call Trusted Advisor-related actions, none of the "trustedadvisor:*" actions restrict your access. The "trustedadvisor:*" actions apply only to Trusted Advisor in the AWS Management Console.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAttachmentsToSet	Grants permission to add one or more attachments to an AWS Support case	Write			
AddCommunicationToCase	Grants permission to add a customer communication to an AWS Support case	Write			
CreateCase	Grants permission to creates a new AWS Support case	Write			
DescribeAttachment	Grants permission to describe attachment detail	Read			
DescribeCaseAttributes	Grants permission to allow secondary services to read AWS Support case attributes.This is an internally managed function	Read			
DescribeCaseOptions	Grants permission to describe the available options for a single AWS Support case. This is an internally managed function	Read			
DescribeCases	Grants permission to list AWS Support cases that matches the given inputs	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCommunication	Grants permission to get a single communication and attachments for a single AWS Support case	Read			
DescribeCommunications	Grants permission to list the communications and attachments for one or more AWS Support cases	Read			
DescribeCreateCaseOptions	Grants permission to describes the available options for creating a support case	Read			
DescribeIssueTypes	Grants permission to return issue types for AWS Support cases	Read			
DescribeServices	Grants permission to list AWS services and categories that applies to each service	Read			
DescribeSeverityLevels	Grants permission to list severity levels that can be assigned to an AWS Support case	Read			
DescribeSupportLevel	Grants permission to return the support level for an AWS Account identifier	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSupportedLanguages	Grants permission to describes the available support languages for a given category code, service code and issue type	Read			
DescribeTrustedAdvisorCheckRefreshStatuses	Grants permission to get the status of a Trusted Advisor refresh check based on a list of check identifiers	Read			
DescribeTrustedAdvisorCheckResult	Grants permission to get the results of the Trusted Advisor check that has the specified check identifier	Read			
DescribeTrustedAdvisorCheckSummaries	Grants permission to get the summaries of the results of the Trusted Advisor checks that have the specified check identifiers	Read			
DescribeTrustedAdvisorChecks	Grants permission to get a list of all available Trusted Advisor checks, including name, identifier, category and description	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInteraction	Grants permission to retrieve personalized troubleshooting assistance for account and technical issues for a specific interaction	Read			
InitiateCallForCase	Grants permission to initiate a call on AWS Support Center. This is an internally managed function	Write			
InitiateChatForCase	Grants permission to initiate a chat on AWS Support Center.This is an internally managed function	Write			
InitiateLiveContactForCase	Grants permission to initiate a live contact on AWS Support Center. This is an internally managed function	Write			
ListInteractionEntries	Grants permission to retrieve a list of entries within a specific interaction, including messages, status updates, or other relevant data points	Read			
ListInteractions	Grants permission to retrieve a list of interactions, potentially with filters or pagination	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutCaseAttributes	Grants permission to allow secondary services to attach attributes to AWS Support cases. This is an internally managed function	Write			
RateCaseCommunication	Grants permission to rate an AWS Support case communication	Write			
RefreshTrustedAdvisorCheck	Grants permission to requests a refresh of the Trusted Advisor check that has the specified check identifier	Write			
ResolveCase	Grants permission to resolve an AWS Support case	Write			
ResolveInteraction	Grants permission to mark a specific interaction as resolved by its unique identifier, indicating that the issue has been addressed and no further action is needed	Write			
SearchForCases	Grants permission to return a list of AWS Support cases that matches the given inputs	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInteraction	Grants permission to start a specific interaction to receive personalized troubleshooting assistance for account and technical issues	Write			support:DescribeSupportLevel
UpdateCaseSeverity	Grants permission to update the severity for a single AWS Support case. This is an internally managed function	Write			
UpdateInteraction	Grants permission to update a specific interaction to receive personalized troubleshooting assistance for account and technical issues	Write			

Resource types defined by AWS Support

AWS Support does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Support, specify `"Resource": "*"` in your policy.

Condition keys for AWS Support

Support has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Support App in Slack

AWS Support App in Slack (service prefix: `supportapp`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Support App in Slack

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSlackChannelConfiguration	Grants permission to create a Slack channel configuration for your account	Write			
DeleteAccountAlias	Grants permission to delete an alias from your account	Write			
DeleteSlackChannelConfiguration	Grants permission to delete a Slack channel configuration from your account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSlackWorkspaceConfiguration	Grants permission to delete a Slack workspace configuration from your account	Write			
DescribeSlackChannels [permission only]	Grants permission to list all public Slack channels in a workspace that have invited the AWS Support App	Read			
GetAccountAlias	Grants permission to get the alias for your account	Read			
GetSlackOauthParameters [permission only]	Grants permission to get parameters for the Slack OAuth code, which the AWS Support App uses to authorize the workspace	Read			
ListSlackChannelConfigurations	Grants permission to list all Slack channel configurations for your account	Read			
ListSlackWorkspaceConfigurations	Grants permission to list all Slack workspace configurations for your account	Read			
PutAccountAlias	Grants permission to create or update an alias for your account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RedeemSlackOauthCode [permission only]	Grants permission to redeem the Slack OAuth code, which the AWS Support App uses to authorize the workspace	Write			
RegisterSlackWorkspaceForOrganization	Grants permission to register a Slack workspace for an AWS account that is part of an organization	Write			
UpdateSlackChannelConfiguration	Grants permission to update a Slack channel configuration for your account	Write			

Resource types defined by AWS Support App in Slack

AWS Support App in Slack does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Support App in Slack, specify `"Resource": "*"` in your policy.

Condition keys for AWS Support App in Slack

Support App has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Support Console

AWS Support Console (service prefix: `support-console`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Support Console

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckSubscription [permission only]	Grants permission to check whether the account has access to given product	Read			
CreateCaseDraft [permission only]	Grants permission to create or update case draft for the given case type	Write			
CreateContact [permission only]	Grants permission to create an authenticated contact for the given contact type	Write			
DeleteCaseDraft	Grants permission to delete a case draft for the given case type	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
DescribeDynamicHelp [permission only]	Grants permission to get dynamic help resources for given service and category	Read			
GetAccountGovCloudEnabled [permission only]	Grants permission to determines whether the calling account is GovCloud enabled	Read			
GetAccountState [permission only]	Grants permission to get the state of the calling account	Read			
GetBanner [permission only]	Grants permission to get the support banner information	Read			
GetCaseDraft [permission only]	Grants permission to get a case draft for given case type	Read			
GetIssueClassificationPredictions [permission only]	Grants permission to get classification predictions of an issue	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIssueTextSummary [permission only]	Grants permission to get a generated text summary of an issue	Read			
GetQuestionnaire [permission only]	Grants permission to get a feedback questionnaire	Read			
SaveFeedback [permission only]	Grants permission to save questionnaire feedback	Write			

Resource types defined by AWS Support Console

AWS Support Console does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Support Console, specify `"Resource": "*"` in your policy.

Condition keys for AWS Support Console

Support Console has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Support Plans

AWS Support Plans (service prefix: `supportplans`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.

- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Support Plans

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSupportPlanSchedule [permission only]	Grants permission to create support plan schedules for this AWS account	Write			
GetSupportPlan [permission only]	Grants permission to view details about the current support plan for this AWS account	Read			
GetSupportPlanUpdateStatus [permission only]	Grants permission to view details about the status for a request to update a support plan	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSupportPlanModifiers [permission only]	Grants permission to view a list of all support plan modifiers for this AWS account	List			
StartSupportPlanUpdate [permission only]	Grants permission to update the support plan for this AWS account	Write			

Resource types defined by AWS Support Plans

AWS Support Plans does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Support Plans, specify `"Resource": "*"` in your policy.

Condition keys for AWS Support Plans

Support Plans has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Sustainability

AWS Sustainability (service prefix: `sustainability`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Sustainability

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCarbon Footprint Summary	Grants permission to view the carbon footprint tool	Read			

Resource types defined by AWS Sustainability

AWS Sustainability does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Sustainability, specify `"Resource": "*"` in your policy.

Condition keys for AWS Sustainability

Sustainability has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Systems Manager

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToResource	Grants permission to add or overwrite one or more tags for a specified AWS 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 AWS 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 AWS accounts in the AWS 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 AWS 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 AWS 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		ssm:InventoryTypeName	
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 AWS 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-execution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			document*		
			automation-definition		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ssm:DocumentVersion	
StartChangeRequestExecution	Grants permission to initiate the execution of an Automation Change Template document	Write	automation-execution*		
			document*		
			automation-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ssm:AutoApprove ssm:DocumentVersion	
StartExecutionPreview	Grants permission to create a preview showing the effects that running a specified Automation runbook would have on the targeted resources	Read			
StartSession	Grants permission to initiate a connection to a specified target for a Session Manager session	Write	document		
			instance		
			managed-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			instance		
			managed-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
UpdateDocumentDefaultVersion	Grants permission to change the default version of an SSM document	Write	document*		
				ssm:DocumentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
UpdateInstanceInformation	Grants permission to SSM Agent to send a heartbeat signal to the Systems Manager service in the cloud	Write	instance		
			managed-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				ssm:resourceTag/tag-key	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS account	Write	servicesetting*		

Resource types defined by AWS 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}:${VersionId}	ssm:DocumentType
bucket	arn:${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}	
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}

Resource types	ARN	Condition keys
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}
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

Resource types	ARN	Condition keys
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/${TagKey} ssm:resourceTag/tag-key
task	arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Systems Manager

AWS 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 AWS 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 AWS 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
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	String

Condition keys	Description	Type
	type. Only available in "aws", "aws-cn", and "aws-us-gov" partitions	
ssm:DocumentVersion	Filters access by verifying that a user has permission to access a specific version of a document	ArrayOfString
ssm:InventoryTypeName	Filters access by verifying that a user also has access to the InventoryType specified in the request	ArrayOfString
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 AWS 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 AWS Systems Manager for SAP

AWS Systems Manager for SAP (service prefix: `ssm-sap`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Systems Manager for SAP
- Resource types defined by AWS Systems Manager for SAP
- Condition keys for AWS Systems Manager for SAP

Actions defined by AWS Systems Manager for SAP

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BackupDatabase	Grants permission to perform backup operation on a specified database	Write			
DeleteResourcePermission	Grants permission to delete the SSM for SAP level resource permissions associated with a SSM for SAP database resource	Permissions management			
DeregisterApplication	Grants permission to deregister an SAP application with SSM for SAP	Write	application		
GetApplication	Grants permission to access information about an application registered with SSM for SAP by providing the application ID or application ARN	Read			
GetComponent	Grants permission to access information about a component registered with SSM for SAP by providing the application ID and component ID	Read	component		
GetConfigurationCheckOperation	Grants permission to get the details of a configuration check operation by specifying the operation ID	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDatabase	Grants permission to access information about a database registered with SSM for SAP by providing the application ID, component ID, and database ID	Read			
GetOperation	Grants permission to access information about an operation by providing its operation ID	Read			
GetResourcePermission	Grants permission to get the SSM for SAP level resource permissions associated with a SSM for SAP database resource	Permissions management			
ListApplications	Grants permission to retrieve a list of all applications registered with SSM for SAP under the customer AWS account	List			
ListComponents	Grants permission to retrieve a list of all components in the account of customer, or a specific application	List	application		
ListConfigurationCheckDefinitions	Grants permission to list all configuration check types supported by AWS Systems Manager for SAP	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfigurationCheckOperations	Grants permission to list past configuration check operations	List			
ListDatabases	Grants permission to retrieve a list of all databases in the account of customer, or a specific application	List			
ListOperationEvents	Grants permission to retrieve a list of all operation events in a specified operation	List			
ListOperations	Grants permission to retrieve a list of all operations in the account of customer, additional filters can be applied	List			
ListSubCheckResults	Grants permission to list the sub-check results of a specified configuration check operation	List			
ListSubCheckRuleResults	Grants permission to list the rules of a specified sub-check belonging to a configuration check operation	List			
ListTagsForResource	Grants permission to list the tags on a specified resource ARN	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePermission	Grants permission to add the SSM for SAP level resource permissions associated with a SSM for SAP database resource	Permissions management			
RegisterApplication	Grants permission to registers an SAP application with SSM for SAP	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RestoreDatabase	Grants permission to restore a database from another database	Write			
StartApplication	Grants permission to start a registered SSM for SAP application	Write	application		
StartApplicationRefresh	Grants permission to start an on-demand discovery of a registered SSM for SAP application	Write	application		
StartConfigurationChecks	Grants permission to iniitiate configuration check operations against a specified application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopApplication	Grants permission to stop a registered SSM for SAP application	Write	application		
TagResource	Grants permission to tag a specified resource ARN	Tagging	application		
			component		
			database		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a specified resource ARN	Tagging	application		
			component		
			database		
				aws:TagKeys	
UpdateApplicationSettings	Grants permission to update settings of a registered SSM for SAP application	Write	application		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateHANABackupSettings	Grants permission to update the HANA backup settings of a specified database	Write			

Resource types defined by AWS Systems Manager for SAP

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:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}`	aws:ResourceTag/${TagKey}
component	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/COMPONENT/${ComponentId}`	aws:ResourceTag/${TagKey}
database	`arn:${Partition}:ssm-sap:${Region}:${Account}:${ApplicationType}/${ApplicationId}/DB/${DatabaseId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Systems Manager for SAP

AWS Systems Manager for SAP defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Systems Manager GUI Connect

AWS 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 AWS Systems Manager GUI Connect
- Resource types defined by AWS Systems Manager GUI Connect
- Condition keys for AWS Systems Manager GUI Connect

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	Grants permission to start a GUI Connect connection	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
UpdateConnectionRecordingPreferences	Grants permission to update GUI Connect connection recording preferences	Write			

Resource types defined by AWS Systems Manager GUI Connect

AWS Systems Manager GUI Connect does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Systems Manager GUI Connect, specify `"Resource": "*"` in your policy.

Condition keys for AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager (service prefix: `ssm-incidents`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Systems Manager Incident Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetIncidentFindings	Grants permission to retrieve details about specified findings for an incident record	Read	incident-record*		
			response-plan*		
CreateReplicationSet	Grants permission to create a replication set	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole ssm-incidents:TagResource
CreateResponsePlan	Grants permission to create a response plan	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole ssm-incidents:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTimelineEvent	Grants permission to create a timeline event for an incident record	Write	incident-record*		
			response-plan*		
DeleteIncidentRecord	Grants permission to delete an incident record	Write	incident-record*		
DeleteReplicationSet	Grants permission to delete a replication set	Write	replication-set*		
DeleteResourcePolicy	Grants permission to delete resource policy from a response plan	Permissions management	response-plan*		
DeleteResponsePlan	Grants permission to delete a response plan	Write	response-plan*		
DeleteTimelineEvent	Grants permission to delete a timeline event	Write	incident-record*		
GetIncidentRecord	Grants permission to view the contents of an incident record	Read	incident-record*		
			response-plan*		
GetReplicationSet	Grants permission to view the replication set	Read	replication-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicies	Grants permission to view resource policies of a response plan	Read	response-plan*		
GetResponsePlan	Grants permission to view the contents of a specified response plan	Read	response-plan*		
GetTimelineEvent	Grants permission to view a timeline event	Read	incident-record*		
			response-plan*		
ListIncidentFindings	Grants permission to list findings for an incident record	List	incident-record*		
			response-plan*		
ListIncidentRecords	Grants permission to list the contents of all incident records	List			
ListRelatedItems	Grants permission to list related items of an incident record	List	incident-record*		
			response-plan*		
ListReplicationSets	Grants permission to list all replication sets	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResponsePlans	Grants permission to list all response plans	List			
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	incident-record		
			replication-set		
			response-plan		
ListTimelineEvents	Grants permission to list all timeline events for an incident record	List	incident-record*		
			response-plan*		
PutResourcePolicy	Grants permission to put resource policy on a response plan	Permissions management	response-plan*		
StartIncident	Grants permission to start a new incident using a response plan	Write	response-plan*		
TagResource	Grants permission to add tags to a response plan	Tagging	incident-record		
			replication-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			response-plan		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a response plan	Tagging	incident-record		
			replication-set		
			response-plan		
				aws:TagKeys	
UpdateDeletionProtection	Grants permission to update replication set deletion protection	Write	replication-set*		
UpdateIncidentRecord	Grants permission to update the contents of an incident record	Write	incident-record*		
			response-plan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRelatedItems	Grants permission to update related items of an incident record	Write	incident-record*		
			response-plan*		
UpdateReplicationSet	Grants permission to update a replication set	Write	replication-set*		
UpdateResponsePlan	Grants permission to update the contents of a response plan	Write	response-plan*		iam:PassRole ssm-incidents:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateTimelineEvent	Grants permission to update a timeline event	Write	incident-record*		
			response-plan*		

Resource types defined by AWS Systems Manager Incident 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
response-plan	arn:${Partition}:ssm-incidents::${Account}:response-plan/${ResponsePlan}	aws:ResourceTag/${TagKey}
incident-record	arn:${Partition}:ssm-incidents::${Account}:incident-record/${ResponsePlan}/${IncidentRecord}	aws:ResourceTag/${TagKey}
replication-set	arn:${Partition}:ssm-incidents::${Account}:replication-set/${ReplicationSet}	aws:ResourceTag/${TagKey}

Condition keys for AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Systems Manager Incident Manager Contacts

AWS Systems Manager Incident Manager Contacts (service prefix: `ssm-contacts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Systems Manager Incident Manager Contacts

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptPage	Grants permission to accept a page	Write	page*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateContactChannel	Grants permission to activate a contact's contact channel	Write	contactchannel*		
AssociateContact [permission only]	Grants permission to use a contact in an escalation plan	Permissions management	contact*		
CreateContact	Grants permission to create a contact	Write	contact*		ssm-contacts:AssociateContact
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateContactChannel	Grants permission to create a contact channel for a contact	Write	contact*		
CreateRotation	Grants permission to create a rotation in an on-call schedule	Write	rotation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRotationOverride	Grants permission to create an override for a rotation in an on-call schedule	Write	rotation*		
DeactivateContactChannel	Grants permission to deactivate a contact's contact channel	Write	contactchannel*		
DeleteContact	Grants permission to delete a contact	Write	contact*		
DeleteContactChannel	Grants permission to delete a contact's contact channel	Write	contactchannel*		
DeleteRotation	Grants permission to delete a rotation	Write	rotation*		
DeleteRotationOverride	Grants permission to delete a rotation's rotation override	Write	rotation*		
DescribeEngagement	Grants permission to describe an engagement	Read	engagement*		
DescribePage	Grants permission to describe a page	Read	page*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetContact	Grants permission to get a contact	Read	contact*		
GetContactChannel	Grants permission to get a contact's contact channel	Read	contactchannel*		
GetContactPolicy	Grants permission to get a contact's resource policy	Read	contact*		
GetRotation	Grants permission to retrieve information about an on-call rotation	Read	rotation*		
GetRotationOverride	Grants permission to retrieve information about an override in an on-call rotation	Read	rotation*		
ListContactChannels	Grants permission to list all of a contact's contact channels	List	contact*		
ListContacts	Grants permission to list all contacts	List			
ListEngagements	Grants permission to list all engagements	List			
ListPageReceipts	Grants permission to list all receipts of a page	List	page*		
ListPageResolutions	Grants permission to list the resolution path of an engagement	List	page*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPagesByContact	Grants permission to list all pages sent to a contact	List	contact*		
ListPagesByEngagement	Grants permission to list all pages created in an engagement	List	engagement*		
ListPreviewRotationShifts	Grants permission to retrieve a list of shifts based on rotation configuration parameters	List			
ListRotationOverrides	Grants permission to retrieve a list of overrides currently specified for an on-call rotation	List	rotation*		
ListRotationShifts	Grants permission to retrieve a list of rotation shifts in an on-call schedule	List	rotation*		
ListRotations	Grants permission to retrieve a list of on-call rotations	List			
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	contact		
			rotation		
PutContactPolicy	Grants permission to add a resource policy to a contact	Write	contact*		
SendActivationCode	Grants permission to send the activation code of a contact's contact channel	Write	contactchannel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartEngagement	Grants permission to start an engagement	Write	contact*		
StopEngagement	Grants permission to stop an engagement	Write	engagement*		
TagResource	Grants permission to add tags to the specified resource	Tagging	contact		
			rotation		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	contact		
			rotation		
				aws:TagKeys	
UpdateContact	Grants permission to update a contact	Write	contact*		ssm-contacts:AssociateContact
UpdateContactChannel	Grants permission to update a contact's contact channel	Write	contactchannel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRotation	Grants permission to update the information specified for an on-call rotation	Write	rotation*		

Resource types defined by AWS Systems Manager Incident Manager Contacts

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
contact	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contact/${ContactAlias}`	aws:ResourceTag/${TagKey}
contactchannel	`arn:${Partition}:ssm-contacts:${Region}:${Account}:contactchannel/${ContactAlias}/${ContactChannelId}`	
engagement	`arn:${Partition}:ssm-contacts:${Region}:${Account}:engagement/${ContactAlias}/${EngagementId}`	
page	`arn:${Partition}:ssm-contacts:${Region}:${Account}:page/${ContactAlias}/${PageId}`	

Resource types	ARN	Condition keys
rotation	arn:${Partition}:ssm-contacts:${Region}:${Account}:rotation/${RotationId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Systems Manager Incident Manager Contacts

AWS Systems Manager Incident Manager Contacts defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Systems Manager Quick Setup

AWS Systems Manager Quick Setup (service prefix: ssm-quicksetup) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Systems Manager Quick Setup

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfigurationManager	Grants permission to create a Quick Setup configuration manager resource	Write	configuration-manager*	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteConfigurationManager	Grants permission to delete a configuration manager	Write	configuration-manager*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConfiguration	Grants permission to get Quick Setup configuration	Read	configuration-manager		
GetConfigurationManager	Grants permission to get a configuration manager	Read	configuration-manager*		
GetServiceSettings	Grants permission to get settings configured for Quick Setup in the requesting AWS account and AWS Region	Read			
ListConfigurationManagers	Grants permission to list Quick Setup configuration managers	List			
ListConfigurations	Grants permission to list Quick Setup configurations	List	configuration-manager		
ListQuickSetupTypes	Grants permission to list the available Quick Setup types	Read			
ListTagsForResource	Grants permission to list tags assigned to the resource	Read	configuration-manager*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to Assign key-value pairs of metadata to AWS resources	Tagging	configuration-manager*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	configuration-manager*		
				aws:TagKeys	
UpdateConfigurationDefinition	Grants permission to update a Quick Setup configuration definition	Write	configuration-manager*		
UpdateConfigurationManager	Grants permission to update a Quick Setup configuration manager	Write	configuration-manager*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceSettings	Grants permission to update settings configured for Quick Setup	Write			

Resource types defined by AWS Systems Manager Quick Setup

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-manager	`arn:${Partition}:ssm-quicksetup:${Region}:${Account}:configuration-manager/${ConfigurationManagerId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Systems Manager Quick Setup

AWS Systems Manager Quick Setup defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Tag Editor

Tag Editor (service prefix: `resource-explorer`) 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 Tag Editor
- Resource types defined by Tag Editor
- Condition keys for Tag Editor

Actions defined by Tag Editor

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceTypes [permission only]	Grants permission to retrieve the resource types currently supported by Tag Editor	List			
ListResources [permission only]	Grants permission to retrieve the identifiers of the resources in the AWS account	List			
ListTags [permission only]	Grants permission to retrieve the tags attached to the specified resource identifiers	Read			tag:GetResources

Resource types defined by Tag Editor

Tag Editor does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Tag Editor, specify `"Resource": "*"` in your policy.

Condition keys for Tag Editor

Tag Editor has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Tax Settings

AWS Tax Settings (service prefix: `tax`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Tax Settings

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteTaxRegistration	Grants permission to batch delete tax registration data	Write			
BatchPutTaxRegistration	Grants permission to batch update tax registrations	Write			
CancelDocument	Grants permission to cancel documents such as withholding slips	Write			
CreateDocument	Grants permission to upload new documents such as withholding slips	Write			
DeleteSupplemental	Grants permission to delete supplemental tax registration data	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TaxRegistration					
DeleteTaxRegistration	Grants permission to delete tax registration data	Write			
GetDocument	Grants permission to retrieve documents such as withholding slips	Read			
GetDocumentUploadUrl	Grants permission to retrieve a generated URL to upload documents	Read			
GetExemptions	Grants permission to view tax exemptions data	Read			
GetTaxInfoReportingDocument [permission only]	Grants permission to view/download tax documents/forms	Read			
GetTaxInheritance	Grants permission to view tax inheritance status	Read			
GetTaxInterview [permission only]	Grants permission to retrieve tax interview data	Read			
GetTaxRegistration	Grants permission to view tax registrations data	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTaxRegistrationDocument	Grants permission to download tax registration documents	Read			
ListDocuments	Grants permission to view documents such as withholding slips	Read			
ListSupplementalTaxRegistrations	Grants permission to view supplemental tax registrations	Read			
ListTaxRegistrations	Grants permission to view tax registrations	Read			
ListWithholdingEligibleInvoices	Grants permission to view eligible withholding invoices	Read			
PutSupplementalTaxRegistration	Grants permission to update supplemental tax registrations data	Write			
PutTaxInheritance	Grants permission to set tax inheritance	Write			
PutTaxInterview [permission only]	Grants permission to update tax interview data	Write			
PutTaxRegistration	Grants permission to update tax registrations data	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExemptions	Grants permission to update tax exemptions data	Write			

Resource types defined by AWS Tax Settings

AWS Tax Settings does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Tax Settings, specify `"Resource": "*"` in your policy.

Condition keys for AWS Tax Settings

Tax Settings has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Telco Network Builder

AWS Telco Network Builder (service prefix: `tnb`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Telco Network Builder
- Resource types defined by AWS Telco Network Builder
- Condition keys for AWS Telco Network Builder

Actions defined by AWS Telco Network Builder

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelSolNetworkOperation	Grants permission to cancel a network operation	Write	network-operation*		
CreateSolFunctionPackage	Grants permission to create a function package	Write	function-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSolNetworkInstance	Grants permission to create a network instance	Write	network-instance*		
			network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSolNetworkPackage	Grants permission to create a network package	Write	network-package*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSolFunctionPackage	Grants permission to delete a function package	Write	function-package*		
DeleteSolNetworkInstance	Grants permission to delete a network instance	Write	network-instance*		
DeleteSolNetworkPackage	Grants permission to delete a network package	Write	network-package*		
GetSolFunctionInstance	Grants permission to get a function instance	Read	function-instance*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackage	Grants permission to get a function package	Read	function-package*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageContent	Grants permission to get a function package contents	Read	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolFunctionPackageDescriptor	Grants permission to get a function package descriptor	Read	function-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkInstance	Grants permission to get a network instance	Read	network-instance*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkOperation	Grants permission to get a network operation	Read	network-operation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackage	Grants permission to get a network package	Read	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageContent	Grants permission to get a network package contents	Read	network-package*		
				aws:ResourceTag/${TagKey}	
GetSolNetworkPackageDescriptor	Grants permission to get a network package descriptor	Read	network-package*		
				aws:ResourceTag/${TagKey}	
InstantiateSolNetworkInstance	Grants permission to instantiate a network instance	Write	network-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ListSolFunctionInstances	Grants permission to list function instances	List	function-instance*		
				aws:ResourceTag/${TagKey}	
ListSolFunctionPackages	Grants permission to list function packages	List	function-package*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkInstances	Grants permission to list network instances	List	network-instance*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSolNetworkOperations	Grants permission to list network operations	List	network-operation*		
				aws:ResourceTag/${TagKey}	
ListSolNetworkPackages	Grants permission to list network packages	List	network-package*		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Grants permission to return a list of tags for a resource	List			
PutSolFunctionPackageContent	Grants permission to upload function package content	Write	function-package*		
PutSolNetworkPackageContent	Grants permission to upload network package content	Write	network-package*		
TagResource	Grants permission to add tags to the specified resource	Tagging	function-instance		
			function-package		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateSolNetworkInstance	Grants permission to terminate a network instance	Write	network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	function-instance		
			function-package		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-instance		
			network-operation		
			network-package		
				aws:TagKeys	
UpdateSolFunctionPackage	Grants permission to update a function package	Write	function-package*		
UpdateSolNetworkInstance	Grants permission to update a network instance	Write	function-instance*		
			network-instance*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSolNetworkPackage	Grants permission to update a network package	Write	network-package*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateSolFunctionPackageContent	Grants permission to validate function package content	Write	function-package*		
ValidateSolNetworkPackageContent	Grants permission to validate network package content	Write	network-package*		

Resource types defined by AWS Telco Network 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
function-package	`arn:${Partition}:tnb:${Region}:${Account}:function-package/${FunctionPackageId}`	aws:ResourceTag/${TagKey}
network-package	`arn:${Partition}:tnb:${Region}:${Account}:network-package/${NetworkPackageId}`	aws:ResourceTag/${TagKey}
network-instance	`arn:${Partition}:tnb:${Region}:${Account}:network-instance/${NetworkInstanceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
function-instance	arn:${Partition}:tnb:${Region}:${Account}:function-instance/${FunctionInstanceId}	aws:ResourceTag/${TagKey}
network-operation	arn:${Partition}:tnb:${Region}:${Account}:network-operation/${NetworkOperationId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Telco Network Builder

AWS Telco Network Builder defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by checking the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by checking tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Textract

Amazon Textract (service prefix: textract) 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 Textract

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AnalyzeDocument	Grants permission to detect instances of real-world document entities within an image provided as input	Read			s3:GetObject
AnalyzeExpense	Grants permission to detect instances of real-world document entities within an image provided as input	Read			s3:GetObject
AnalyzeID	Grants permission to detect relevant information from	Read			s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	identity documents provided as input				
CreateAdapter	Grants permission to create an Amazon Textract adapter	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAdapterVersion	Grants permission to create an Amazon Textract adapter version	Write	adapter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAdapter	Grants permission to delete an Amazon Textract adapter	Write	adapter*		
DeleteAdapterVersion	Grants permission to delete an Amazon Textract adapter version	Write	adapterversion*		
DetectDocumentText	Grants permission to detect text in document images	Read			s3:GetObject
GetAdapter	Grants permission to get an Amazon Textract adapter	Read	adapter*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAdapterVersion	Grants permission to get an Amazon Textract adapter version	Read	adapterversion*		
GetDocumentAnalysis	Grants permission to return information about a document analysis job	Read			
GetDocumentTextDetection	Grants permission to return information about a document text detection job	Read			
GetExpenseAnalysis	Grants permission to return information about an expense analysis job	Read			
GetLendingAnalysis	Grants permission to retrieve page-level information regarding a lending analysis job	Read			
GetLendingAnalysisSummary	Grants permission to retrieve summarized information regarding a lending analysis job	Read			
ListAdapterVersions	Grants permission to list Amazon Textract adapter versions	Read			
ListAdapters	Grants permission to list Amazon Textract adapters	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to return a list of tags associated with a resource	Read	adapter		
			adapterversion		
StartDocumentAnalysis	Grants permission to start an asynchronous job to detect instances of real-world document entities within an image or pdf provided as input	Write			s3:GetObject
StartDocumentTextDetection	Grants permission to start an asynchronous job to detect text in document images or pdfs	Write			s3:GetObject
StartExpenseAnalysis	Grants permission to start an asynchronous job to detect instances of invoices or receipts within an image or pdf provided as input	Write			s3:GetObject
StartLendingAnalysis	Grants permission to start an asynchronous job for detection of entities in a lending document, takes a provided image or PDF as input	Write			s3:GetObject
TagResource	Grants permission to add one or more tags to a resource	Tagging	adapter		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			adapterversion		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	adapter		
			adapterversion		
				aws:TagKeys	
UpdateAdapter	Grants permission to update Amazon Textract adapter	Write	adapter*		

Resource types defined by Amazon Textract

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
adapter	arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}	aws:ResourceTag/${TagKey}
adapterversion	arn:${Partition}:textract:${Region}:${Account}:/adapters/${AdapterId}/versions/${AdapterVersion}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Textract

Amazon Textract defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Timestream

Amazon Timestream (service prefix: timestream) 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelQuery	Grants permission to cancel queries in your account	Write			timestream:DescribeEndpoints
CreateBatchLoadTask	Grants permission to create a batch load task in your account	Write	table*		timestream:DescribeEndpoints timestream:WriteRecords
CreateDatabase	Grants permission to create a database in your account	Write	database*		timestream:Describ

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					eEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScheduledQuery	Grants permission to create a scheduled query in your account	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole timestream:DescribeEndpoints
CreateTable	Grants permission to create a table in your account	Write	table*		timestream:DescribeEndpoints
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDatabase	Grants permission to delete a database in your account	Write	database*		timestream:DescribeEndpoints
DeleteScheduledQuery	Grants permission to delete a scheduled query in your account	Write	scheduled-query*		timestream:DescribeEndpoints
DeleteTable	Grants permission to delete a table in your account	Write	table*		timestream:DescribeEndpoints
DescribeAccountSettings	Grants permission to describe your account settings	Read			timestream:DescribeEndpoints
DescribeBatchLoadTask	Grants permission to describe a batch load task in your account	Read			timestream:DescribeEndpoints
DescribeDatabase	Grants permission to describe a database in your account	Read	database*		timestream:DescribeEndpoints
DescribeEndpoints	Grants permission to describe timestream endpoints	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScheduledQuery	Grants permission to describe a scheduled query in your account	Read	scheduled-query*		timestream:DescribeEndpoints
DescribeTable	Grants permission to describe a table in your account	Read	table*		timestream:DescribeEndpoints
ExecuteScheduledQuery	Grants permission to execute a scheduled query in your account	Write	scheduled-query*		timestream:DescribeEndpoints
GetAwsBackupStatus	Grants permission to get Status of a Timestream Table Backup	Read			timestream:DescribeEndpoints
GetAwsRestoreStatus	Grants permission to get Status of a Timestream Table Restore	Read			timestream:DescribeEndpoints
ListBatchLoadTasks	Grants permission to list batch load tasks in your account	List			timestream:DescribeEndpoints

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatabases	Grants permission to list databases in your account	List			timestream:DescribeEndpoints
ListMeasures	Grants permission to list measures of a table in your account	List	table*		timestream:DescribeEndpoints
ListScheduledQueries	Grants permission to list scheduled queries in your account	List			timestream:DescribeEndpoints
ListTables	Grants permission to list tables in your account	List	database*		timestream:DescribeEndpoints
ListTagsForResource	Grants permission to list tags of a resource in your account	Read	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PrepareQuery	Grants permission to issue prepare queries	Read	table*		timestream:DescribeEndpoints timestream:Select
ResumeBatchLoadTask	Grants permission to resume a batch load task in your account	Write			timestream:DescribeEndpoints timestream:WriteRecords
Select	Grants permission to issue 'select from table' queries	Read	table*		timestream:DescribeEndpoints
SelectValues	Grants permission to issue 'select 1' queries	Read			timestream:DescribeEndpoints
StartAwsBackupJob	Grants permission to start a Backup Job for a Timestream Table	Write	table*		timestream:DescribeEndpoints

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartAwsRestoreJob	Grants permission to start Restore Job for a Backup of Timestream Table	Write	table*		timestream:DescribeEndpoints
TagResource	Grants permission to add tags to a resource	Tagging	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Unload	Grants permission to issue Unload queries	Write	table*		s3:AbortMultipartUpload s3:GetObject s3:PutObject timestream:DescribeEndpoints timestream:Select
UntagResource	Grants permission to remove a tag from a resource	Tagging	database*		timestream:DescribeEndpoints
			scheduled-query*		
			table*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountSettings	Grants permission to update your account settings	Write			timestream:DescribeEndpoints
UpdateDatabase	Grants permission to update a database in your account	Write	database*		timestream:DescribeEndpoints
UpdateScheduledQuery	Grants permission to update a scheduled query in your account	Write	scheduled-query*		timestream:DescribeEndpoints
UpdateTable	Grants permission to update a table in your account	Write	table*		timestream:DescribeEndpoints
WriteRecords	Grants permission to ingest data to a table in your account	Write	table*		timestream:DescribeEndpoints

Resource types defined by Amazon Timestream

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:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}	aws:ResourceTag/${TagKey}
table	arn:${Partition}:timestream:${Region}:${Account}:database/${DatabaseName}/table/${TableName}	aws:ResourceTag/${TagKey}
scheduled-query	arn:${Partition}:timestream:${Region}:${Account}:scheduled-query/${ScheduledQueryName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Timestream

Amazon Timestream defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDbCluster	Grants permission to create a new Timestream InfluxDB Cluster	Write	db-parameter-group		timestream-influxdb:CreateDbInstance
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateDbInstance	Grants permission to create a new Timestream InfluxDB instance	Write	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	Grants permission to create a new Timestream InfluxDB parameter group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDbCluster	Grants permission to delete a Timestream InfluxDB Cluster	Write	db-cluster*		timestream-influxdb:DeleteDbInstance

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListDbInstancesForCluster	Grants permission to list information about all Timestream InfluxDB Instances belonging to a cluster	Read	db-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
RebootDbCluster	Grants permission to reboot a Timestream InfluxDB Cluster	Write	db-cluster*		timestream-influxdb:RebootDbInstance
			db-instance		
RebootDbInstance	Grants permission to reboot a Timestream InfluxDB instance	Write	db-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a Timestream InfluxDB resource	Tagging	db-cluster		
			db-instance		
			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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String

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 AWS Tiros

AWS Tiros (service prefix: `tiros`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Tiros

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQuery [permission only]	Grants permission to create a VPC reachability query	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExtendQuery [permission only]	Grants permission to extend a VPC reachability query to include the calling principals account	Write			
GetQueryAnswer [permission only]	Grants permission to get VPC reachability query answers	Read			
GetQueryExplanation [permission only]	Grants permission to get VPC reachability query explanations	Read			
GetQueryExtensionAccounts [permission only]	Grants permission to list accounts that might be useful in a new query	Read			

Resource types defined by AWS Tiros

AWS Tiros does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Tiros, specify `"Resource": "*"` in your policy.

Condition keys for AWS Tiros

Tiros has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateLanguageModel	Grants permission to create a new custom language model	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject 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/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:ResourceTag/${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/${TagKey} aws:ResourceTag/${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 AWS 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/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	Grants permission to start a bidirectional HTTP2 stream where audio is streamed to AWS HealthScribe and the transcription results are streamed to your application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMedicalStreamTranscription	Grants permission to start a protocol where audio is streamed to Transcribe Medical and the transcription results are streamed to your application	Write			
StartMedicalStreamTranscriptionWebSocket	Grants permission to start a WebSocket 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
StartMedicalTranscriptionJob	Grants permission to start an asynchronous job to transcribe medical speech to text	Write		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:ResourceTag/${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/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource with given key value pairs	Tagging		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:TagKeys	
UntagResource	Grants permission to untag a resource with given key	Tagging		aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS 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, provided in the form of a KMS key ARN	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 AWS Transfer Family

AWS Transfer Family (service prefix: `transfer`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Transfer Family

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccess	Grants permission to add an access associated with a server	Write	server*		iam:PassRole
CreateAgreement	Grants permission to add an agreement associated with a server	Write	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateConnector	Grants permission to create a connector	Write	profile		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transfer:RequestConnectorProtocol	
CreateProfile	Grants permission to create a profile	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServer	Grants permission to create a server	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transfer:RequestServerEndpointType transfer:RequestServerDomain transfer:RequestServerProtocols	iam:PassRole
CreateUser	Grants permission to add a user associated with a server	Write	server*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateWebApp	Grants permission to create a webapp	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflow	Grants permission to create a workflow	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteAccess	Grants permission to delete access	Write	server*		
DeleteAgreement	Grants permission to delete agreement	Write	agreement*		
DeleteCertificate	Grants permission to delete certificate	Write	certificate*		
DeleteConnector	Grants permission to delete connector	Write	connector*		
DeleteHostKey	Grants permission to delete a host key associated with a server	Write	host-key*		
DeleteProfile	Grants permission to delete profile	Write	profile*		
DeleteServer	Grants permission to delete a server	Write	server*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSshPublicKey	Grants permission to delete an SSH public key from a user	Write	user*		
DeleteUser	Grants permission to delete a user associated with a server	Write	user*		
DeleteWebApp	Grants permission to delete webapp	Write	webapp*		
DeleteWebAppCustomization	Grants permission to delete webapp customization	Write	webapp*		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow*		
DescribeAccess	Grants permission to describe an access assigned to a server	Read	server*		
DescribeAgreement	Grants permission to describe an agreement assigned to a server	Read	agreement*		
DescribeCertificate	Grants permission to describe a certificate	Read	certificate*		
DescribeConnector	Grants permission to describe a connector	Read	connector*		
DescribeExecution	Grants permission to describe an execution associated with a workflow	Read	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeHostKey	Grants permission to describe a host key associated with a server	Read	host-key*		
DescribeProfile	Grants permission to describe a profile	Read	profile*		
DescribeSecurityPolicy	Grants permission to describe a security policy	Read			
DescribeServer	Grants permission to describe a server	Read	server*		
DescribeUser	Grants permission to describe a user associated with a server	Read	user*		
DescribeWebApp	Grants permission to describe a webapp	Read	webapp*		
DescribeWebAppCustomization	Grants permission to describe a webapp customization	Read	webapp*		
DescribeWorkflow	Grants permission to describe a workflow	Read	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportCertificate	Grants permission to add a certificate	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
ImportHostKey	Grants permission to add a host key to a server	Write	server*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
ImportSshPublicKey	Grants permission to add an SSH public key to a user	Write	user*		
ListAccesses	Grants permission to list accesses	Read	server*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAgreements	Grants permission to list agreements	Read	server*		
ListCertificates	Grants permission to list certificates	Read			
ListConnectors	Grants permission to list connectors	Read			
ListExecutions	Grants permission to list executions associated with a workflow	Read	workflow*		
ListFileTransferResults	Grants permission to list file transfer statuses for connectors	Read	connector*		
ListHostKeys	Grants permission to list host keys associated with a server	Read	server*		
ListProfiles	Grants permission to list profiles	Read			
ListSecurityPolicies	Grants permission to list security policies	List			
ListServers	Grants permission to list servers	List			
ListTagsForResource	Grants permission to list tags for an AWS Transfer Family resource	Read	agreement		
			certificate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	Grants permission to list users associated with a server	List	server*		
ListWebApps	Grants permission to list webapps	List			
ListWorkflows	Grants permission to list workflows	List			
SendWorkflowStepState	Grants permission to send a callback for asynchronous custom steps	Write	workflow*		
StartDirectoryListing	Grants permission to initiate a list operation on a remote server using a connector	Write	connector*		
StartFileTransfer	Grants permission to initiate a connector file transfer	Write	connector*		
StartRemoteDelete	Grants permission to initiate a connector delete operation on remote server	Write	connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartRemoteMove	Grants permission to initiate a connector move operation on remote server	Write	connector*		
StartServer	Grants permission to start a server	Write	server*		
StopServer	Grants permission to stop a server	Write	server*		
TagResource	Grants permission to tag an AWS Transfer Family resource	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	Grants permission to test a connector's connection to remote server	Write	connector*		
TestIdentityProvider	Grants permission to test a server's custom identity provider	Read	user*		
UntagResource	Grants permission to untag an AWS Transfer Family resource	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAccess	Grants permission to update access	Write			iam:PassRole
UpdateAgreement	Grants permission to update an agreement	Write	agreement*		iam:PassRole
UpdateCertificate	Grants permission to update a certificate	Write	certificate*		
UpdateConnector	Grants permission to update a connector	Write	connector*		iam:PassRole
			profile		
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
				transfer:RequestServerEndpointType transfer:RequestServerProtocols	
UpdateUser	Grants permission to update the configuration of a user	Write	user*		iam:PassRole
UpdateWebApp	Grants permission to update the configuration of a webapp	Write	webapp*		iam:PassRole
UpdateWebAppCustomization	Grants permission to update the configuration of a webapp cutomization	Write	webapp*		iam:PassRole

Resource types defined by AWS Transfer Family

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
user	arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}	aws:ResourceTag/${TagKey}
server	arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}	aws:ResourceTag/${TagKey}
certificate	arn:${Partition}:transfer:${Region}:${Account}:certificate/${CertificateId}	aws:ResourceTag/${TagKey}
connector	arn:${Partition}:transfer:${Region}:${Account}:connector/${ConnectorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:transfer:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
agreement	arn:${Partition}:transfer:${Region}:${Account}:agreement/${ServerId}/${AgreementId}	aws:ResourceTag/${TagKey}
host-key	arn:${Partition}:transfer:${Region}:${Account}:host-key/${ServerId}/${HostKeyId}	aws:ResourceTag/${TagKey}
webapp	arn:${Partition}:transfer:${Region}:${Account}:webapp/${WebAppId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Transfer Family

AWS Transfer Family defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the

policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
transfer:RequestConnectorProtocol	Filters access by the connector protocol that is passed in the request	String
transfer:RequestServerDomain	Filters access by the storage domain that is passed in the request	String
transfer:RequestServerEndpointType	Filters access by the endpoint type that is passed in the request	String
transfer:RequestServerProtocols	Filters access by the server protocols that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Transform

AWS Transform (service prefix: `transform`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Transform

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Connector Resource [permission only]	Grants permission to invoke AssociateConnectorResource on AWS Transform	Write	connector*		
CreateProfile [permission only]	Grants permission to invoke CreateProfile on AWS Transform	Write	profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAgentRuntimeConfiguration [permission only]	Grants permission to invoke DeleteAgentRuntimeConfiguration on AWS Transform	Write			
DeleteConnector [permission only]	Grants permission to invoke DeleteConnector on AWS Transform	Write	connector*		
DeleteProfile [permission only]	Grants permission to invoke DeleteProfile on AWS Transform	Write	profile*		
GetAccountSettings [permission only]	Grants permission to invoke GetAccountSettings on AWS Transform	Read			
GetAgent [permission only]	Grants permission to invoke GetAgent on AWS Transform	Read			
GetAgentRuntimeConfiguration [permission only]	Grants permission to invoke GetAgentRuntimeConfiguration on AWS Transform	Read			
GetConnector [permission only]	Grants permission to invoke GetConnector on AWS Transform	Read	connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAgents [permission only]	Grants permission to invoke ListAgents on AWS Transform	Read			
ListConnectors [permission only]	Grants permission to invoke ListConnectors on AWS Transform	List			
ListProfiles [permission only]	Grants permission to invoke ListProfiles on AWS Transform	List			
ListTagsForResource [permission only]	Grants permission to invoke ListTagsForResource on AWS Transform	Read	connector*		
PutAgentRuntimeConfiguration [permission only]	Grants permission to invoke PutAgentRuntimeConfiguration on AWS Transform	Write			
RejectConnector [permission only]	Grants permission to invoke RejectConnector on AWS Transform	Write	connector*		
TagResource [permission only]	Grants permission to invoke TagResource on AWS Transform	Tagging	connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [permission only]	Grants permission to invoke UntagResource on AWS Transform	Tagging	connector*		
				aws:TagKeys	
UpdateAccountSettings [permission only]	Grants permission to invoke UpdateAccountSettings on AWS Transform	Write			
UpdateAgentAccess [permission only]	Grants permission to invoke UpdateAgentAccess on AWS Transform	Write			
UpdateProfile [permission only]	Grants permission to invoke UpdateProfile on AWS Transform	Write	profile*		

Resource types defined by AWS Transform

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:${Partition}:transform:${Region}:${Account}:profile/${Identifier}`	
connector	`arn:${Partition}:transform:${Region}:${Account}:connector/${WorkspaceId}/${ConnectorId}`	

Condition keys for AWS Transform

AWS Transform defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Transform custom

AWS Transform custom (service prefix: `transform-custom`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Transform custom

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteTransformationPackageUpload	Grants permission to invoke CompleteTransformationPackageUpload on AWS Transform custom	Write	package*		
				aws:ResourceTag/${TagKey}	
ConverseStream	Grants permission to invoke ConverseStream on AWS Transform custom	Write			
CreateCampaign	Grants permission to invoke CreateCampaign on AWS Transform custom	Write	campaign*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
CreateTransformationPackageUrl	Grants permission to invoke CreateTransformationPackageUrl on AWS Transform custom	Write	package*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteCampaign	Grants permission to invoke DeleteCampaign on AWS Transform custom	Write	campaign*		
				aws:ResourceTag/${TagKey}	
DeleteKnowledgeItem	Grants permission to invoke DeleteKnowledgeItem on AWS Transform custom	Write	knowledge-item*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteTransformationPackage	Grants permission to invoke DeleteTransformationPackage on AWS Transform custom	Write	package*		
				aws:ResourceTag/${TagKey}	
ExecuteTransformation	Grants permission to invoke ExecuteTransformation on AWS Transform custom	Write	package*		
				aws:ResourceTag/${TagKey}	
GetCampaign	Grants permission to invoke GetCampaign on AWS Transform custom	Read	campaign*		
				aws:ResourceTag/${TagKey}	
GetKnowledgeItem	Grants permission to invoke GetKnowledgeItem on AWS Transform custom	Read	knowledge-item*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransformationPackageUrl	Grants permission to invoke GetTransformationPackageUrl on AWS Transform custom	Read	package*		
				aws:ResourceTag/${TagKey}	
ListCampaignRepositories	Grants permission to invoke ListCampaignRepositories on AWS Transform custom	Read	campaign*		
				aws:ResourceTag/${TagKey}	
ListCampaigns	Grants permission to invoke ListCampaign on AWS Transform custom	List			
ListKnowledgeItems	Grants permission to invoke ListKnowledgeItems on AWS Transform custom	List			
ListTagsForResource	Grants permission to invoke ListTagsForResource on AWS Transform custom	Read			
ListTransformationPackageMetadata	Grants permission to invoke ListTransformationPackageMetadata on AWS Transform custom	List			
TagResource	Grants permission to invoke TagResource on AWS Transform custom	Tagging	campaign		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			knowledge-item		
			package		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to invoke UntagResource on AWS Transform custom	Tagging	campaign		
			knowledge-item		
			package		
				aws:TagKeys	
UpdateCampaign	Grants permission to invoke UpdateCampaign on AWS Transform custom	Write	campaign*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCampaignRepositoryStatus	Grants permission to invoke UpdateCampaignRepositories on AWS Transform custom	Write	campaign*		
				aws:ResourceTag/${TagKey}	
UpdateKnowledgeItemConfiguration	Grants permission to invoke UpdateKnowledgeItemConfiguration on AWS Transform custom	Write	package*		
				aws:ResourceTag/${TagKey}	
UpdateKnowledgeItemStatus	Grants permission to invoke UpdateKnowledgeItemStatus on AWS Transform custom	Write	knowledge-item*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS Transform custom

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
campaign	arn:${Partition}:transform-custom:${Region}:${Account}:campaign/${Name}	aws:ResourceTag/${TagKey}
knowledge-item	arn:${Partition}:transform-custom:${Region}:${Account}:package/${TransformationPackageName}/knowledge-item/${Id}	aws:ResourceTag/${TagKey}
package	arn:${Partition}:transform-custom:${Region}:${Account}:package/${Name}	aws:ResourceTag/${TagKey}

Condition keys for AWS Transform custom

AWS Transform custom defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Translate

Amazon Translate (service prefix: `translate`) 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 Translate

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateParallelData	Grants permission to create a Parallel Data	Write	parallel-data		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteParallelData	Grants permission to delete a Parallel Data	Write	parallel-data		
DeleteTerminology	Grants permission to delete a terminology	Write	terminology		
DescribeTextTranslationJob	Grants permission to get the properties associated with an asynchronous batch translation job	Read			
GetParallelData	Grants permission to get a Parallel Data	Read	parallel-data		
GetTerminology	Grants permission to retrieve a terminology	Read	terminology		
ImportTerminology	Grants permission to create or update a terminology, depending on whether or not one already exists for the given terminology name	Write	terminology		
				aws:RequestTag/${TagKey} aws:TagKeys	
ListLanguages	Grants permission to list supported languages	List			
ListParallelData	Grants permission to list Parallel Data associated with your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a resource	Read	parallel-data		
			terminology		
ListTerminologies	Grants permission to list terminologies associated with your account	List			
ListTextTranslationJobs	Grants permission to list batch translation jobs that you have submitted	List			
StartTextTranslationJob	Grants permission to start an asynchronous batch translation job. Batch translation jobs can be used to translate large volumes of text across multiple documents at once	Write	parallel-data		
			terminology		
StopTextTranslationJob	Grants permission to stop an asynchronous batch translation job that is in progress	Write			
TagResource	Grants permission to tag a resource with given key value pairs	Tagging	parallel-data		
			terminology		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
TranslateDocument	Grants permission to translate a document from a source language to a target language	Read	terminology		
TranslateText	Grants permission to translate text from a source language to a target language	Read	parallel-data		
			terminology		
UntagResource	Grants permission to untag a resource with given key	Tagging	parallel-data		
			terminology		
				aws:TagKeys	
UpdateParallelData	Grants permission to update an existing Parallel Data	Write	parallel-data		

Resource types defined by Amazon Translate

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
terminology	`arn:${Partition}:translate:${Region}:${Account}:terminology/${ResourceName}`	aws:ResourceTag/${TagKey}
parallel-data	`arn:${Partition}:translate:${Region}:${Account}:parallel-data/${ResourceName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Translate

Amazon Translate defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by requiring tag values present in a resource creation request	String
aws:ResourceTag/${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

Actions, resources, and condition keys for AWS Trusted Advisor

AWS 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 AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

The 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 AWS Support API.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateRecommendationRe	Grants permission to update one or more exclusion status	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
sourceExclusion	for a list of recommendation resources				
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 AWS Support plan and various AWS Trusted Advisor preferences	Read			
DescribeAccountAccess [permission only]	Grants permission to view if the AWS account has enabled or disabled AWS Trusted Advisor	Read			
DescribeCheckItems	Grants permission to view details for the check items	Read	checks*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCheckRefreshStatuses	Grants permission to view the refresh statuses for AWS 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 AWS Trusted Advisor check summaries	Read	checks*		
DescribeChecks	Grants permission to view details for AWS Trusted Advisor checks	Read			
DescribeNotificationConfigurations	Grants permission to get your email notification preferences for Trusted Advisor Priority	Read			
DescribeNotificationPreferences [permission only]	Grants permission to view the notification preferences for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrganization [permission only]	Grants permission to view if the AWS account meets the requirements to enable the organizational view feature	Read			
DescribeOrganizationAccounts [permission only]	Grants permission to view the linked AWS 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 AWS Trusted Advisor Priority	Read			
DescribeRiskResources	Grants permission to view affected resources for a risk in AWS Trusted Advisor Priority	Read			
DescribeRisks	Grants permission to view risks in AWS Trusted Advisor Priority	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServiceMetadata [permission only]	Grants permission to view information about organizational view reports, such as the AWS Regions, check categories, check names, and resource statuses	Read			
DownloadRisk	Grants permission to download a file that contains details about the risk in AWS Trusted Advisor Priority	Read			
ExcludeCheckItems [permission only]	Grants permission to exclude recommendations for AWS Trusted Advisor checks	Write	checks*		
GenerateReport [permission only]	Grants permission to create a report for AWS Trusted Advisor checks in your organization	Write			
GetEngagement	Grants permission to view an engagment	Read			
GetEngagementAttachment	Grants permission to view an engagment attachment	Read			
GetEngagementType	Grants permission to view a specific engagement type	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOrganizationRecommendation	Grants permission to get a specific recommendation within an AWS 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 AWS Trusted Advisor checks	Write	checks*		
ListAccountsForParent [permission only]	Grants permission to view, in the Trusted Advisor console, all of the accounts in an AWS organization that are contained by a root or organizational unit (OU)	Read			
ListChecks	Grants permission to list a filterable set of Checks	List			
ListEngagementCommunications	Grants permission to view all communications for an engagement	Read			
ListEngagementTypes	Grants permission to view all engagement types	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEngagements	Grants permission to view all engagements	Read			
ListOrganizationRecommendationAccounts	Grants permission to list the accounts that own the resources for an AWS Organization aggregate recommendation. This API only supports prioritized recommendations	List			
ListOrganizationRecommendationResources	Grants permission to list Resources of a Recommendation within an AWS Organization. This API only supports prioritized recommendations	List			
ListOrganizationRecommendations	Grants permission to list a filterable set of Recommendations within an AWS Organization. This API only supports prioritized recommendations	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS organization	Read			
RefreshCheck	Grants permission to refresh an AWS Trusted Advisor check	Write	checks*		
SetAccountAccess [permission only]	Grants permission to enable or disable AWS Trusted Advisor for the account	Write			
SetOrganizationAccess [permission only]	Grants permission to enable the organizational view feature for AWS 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS Trusted Advisor	Write			
UpdateOrganizationRecommendationLifecycle	Grants permission to update the lifecyle of a Recommendation within an AWS Organization. This API only supports prioritized recommendations	Write			
UpdateRecommendationLifecycle	Grants permission to update the lifecyle of a Recommendation. This API only supports prioritized recommendations	Write			
UpdateRiskStatus	Grants permission to update the risk status in AWS Trusted Advisor Priority	Write			

Resource types defined by AWS 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 AWS 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 AWS global condition context keys.

Actions, resources, and condition keys for AWS User Experience Customization

AWS User Experience Customization (service prefix: `uxc`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS User Experience Customization

- Resource types defined by AWS User Experience Customization
- Condition keys for AWS User Experience Customization

Actions defined by AWS User Experience Customization

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccountColor	Grants permission to delete account color setting	Write			
GetAccountColor	Grants permission to retrieve account color for given account	Read			
GetAccountCustomizations	Grants permission to retrieve account customizations	Read			
ListServices	Grants permission to list available services	Read			
PutAccountColor	Grants permission to set account color	Write			
UpdateAccountCustomizations	Grants permission to update account customizations	Write			

Resource types defined by AWS User Experience Customization

AWS User Experience Customization does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS User Experience Customization, specify `"Resource": "*"` in your policy.

Condition keys for AWS User Experience Customization

User Experience Customization (UXC) has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS User Notifications

AWS User Notifications (service prefix: `notifications`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS User Notifications

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateChannel	Grants permission to associate a new Channel with a particular NotificationConfiguration	Write	NotificationConfiguration*		
AssociateManagedNotificationAccountContact	Grants permission to associate an Account contact to a particular Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
AssociateManagedNotificationAdditionalChannel	Grants permission to associate a Channel to a particular Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
AssociateOrganizationalUnit	Grants permission to associate an Organizational Unit to a particular Notification Configuration	Write	NotificationConfiguration*		
CreateEventRule	Grants permission to create a new EventRule, associating it with a NotificationConfiguration	Write			
CreateNotificationConfiguration	Grants permission to create a NotificationConfiguration	Write		aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
DeleteEventRule	Grants permission to delete an EventRule	Write	EventRule*		
DeleteNotificationConfiguration	Grants permission to delete a NotificationConfiguration	Write	NotificationConfiguration*		
DeregisterNotificationHub	Grants permission to deregister a NotificationHub	Write			
DisableNotificationsAccessForOrganization	Grants permission to disable Service Trust for AWS User Notifications	Permissions management			organizations:DisableAWSServiceAccess
DisassociateChannel	Grants permission to remove a Channel from a NotificationConfiguration	Write	NotificationConfiguration*		
DisassociateManagedNotificationAccountContact	Grants permission to remove an Account contact from a Managed Notification Configuration	Write	ManagedNotificationConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateManagedNotificationAdditionalChannel	Grants permission to remove a Channel from a Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
DisassociateOrganizationalUnit	Grants permission to disassociate an Organizational Unit to a particular Notification Configuration	Write	NotificationConfiguration*		
EnableNotificationsAccessForOrganization	Grants permission to enable Service Trust for AWS User Notifications	Permissions management			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
GetEventRule	Grants permission to get an EventRule	Read	EventRule*		
GetFeatureOptInStatus [permission only]	Grants permission to read the opt-in status of an AWS User Notification Service feature	Read			
GetManagedNotificationChildEvent	Grants permission to get a Managed Notification Child Event	Read	ManagedNotificationChildEvent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetManagedNotificationConfiguration	Grants permission to get a Managed Notification Configuration	Read	ManagedNotificationConfiguration*		
GetManagedNotificationEvent	Grants permission to get a Managed NotificationEvent	Read	ManagedNotificationEvent*		
GetNotificationConfiguration	Grants permission to get a NotificationConfiguration	Read	NotificationConfiguration*		
GetNotificationEvent	Grants permission to get a NotificationEvent	Read	NotificationEvent*		
GetNotificationsAccessForOrganization	Grants permission to read Service Trust for AWS User Notifications	Read			
ListChannels	Grants permission to list Channels by NotificationConfiguration	List	NotificationConfiguration*		
ListEventRules	Grants permission to list EventRules	List			
ListManagedNotificationChannelAssociations	Grants permission to list Account contacts and Channels associated with a Managed Notification Configuration	List	ManagedNotificationConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListManagedNotificationChildEvents	Grants permission to list Managed Notification Child Events	List			
ListManagedNotificationConfigurations	Grants permission to list Managed Notification Configurations	List			
ListManagedNotificationEvents	Grants permission to list Managed Notification Events	List			
ListMemberAccounts	Grants permission to list Member Accounts for a Notification Configuration	List	NotificationConfiguration*		
ListNotificationConfigurations	Grants permission to list NotificationConfigurations	List			
ListNotificationEvents	Grants permission to list NotificationEvents	List			
ListNotificationHubs	Grants permission to list NotificationHubs	List			
ListOrganizationalUnits	Grants permission to list Organizational Units for a Notification Configuration	List	NotificationConfiguration*		
ListTagsForResource	Grants permission to get tags for a resource	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFeatureOptInStatus [permission only]	Grants permission to update the opt-in status of an AWS User Notification Service feature	Write			
RegisterNotificationHub	Grants permission to register a NotificationHub	Write			
TagResource	Grants permission to tag a resource	Tagging	NotificationConfiguration*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	Grants permission to update an EventRule	Write	EventRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotificationConfiguration	Grants permission to update a NotificationConfiguration	Write	NotificationConfiguration*		

Resource types defined by AWS User Notifications

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
EventRule	`arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}/rule/${EventRuleId}`	
NotificationConfiguration	`arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}`	aws:ResourceTag/${TagKey}
NotificationEvent	`arn:${Partition}:notifications:${Region}:${Account}:configuration/${NotificationConfigurationId}/event/${NotificationEventId}`	
ManagedNotificationChildEvent	`arn:${Partition}:notifications::${Account}:managed-notification-configur`	

Resource types	ARN	Condition keys
	ation/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}/child-event/${NotificationChildEventId}	
ManagedNotificationConfiguration	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}	
ManagedNotificationEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}	

Condition keys for AWS User Notifications

AWS User Notifications defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS User Notifications Contacts

AWS User Notifications Contacts (service prefix: `notifications-contacts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS User Notifications Contacts
- Resource types defined by AWS User Notifications Contacts
- Condition keys for AWS User Notifications Contacts

Actions defined by AWS User Notifications Contacts

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateEmailContact	Grants permission to activate the email contact associated with the given ARN if the provided code is valid	Write	EmailContactResource*		
CreateEmailContact	Grants permission to create an email contact	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteEmailContact	Grants permission to delete an email contact associated with the given ARN	Write	EmailContactResource*		
GetEmailContact	Grants permission to get an email contact associated with the given ARN	Read	EmailContactResource*		
ListEmailContacts	Grants permission to list email contacts	List			
ListTagsForResource	Grants permission to get tags for a resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendActivationCode	Grants permission to send an activation link to the email associated with the given ARN	Write	EmailContactResource*		
TagResource	Grants permission to tag a resource	Tagging	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	EmailContactResource*		
				aws:TagKeys	

Resource types defined by AWS User Notifications Contacts

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
EmailContactResource	arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}	aws:ResourceTag/${TagKey}

Condition keys for AWS User Notifications Contacts

AWS User Notifications Contacts defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS User Subscriptions

AWS User Subscriptions (service prefix: user-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 AWS User Subscriptions

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClaim	Grants permission to create a User subscription Claim	Write		user-subscriptions:CreateForSelf	
DeleteClaim	Grants permission to delete a User subscription Claim	Write			
ListApplicationClaims	Grants permission to list all User subscription Claims for Application	List			
ListClaims	Grants permission to list all User subscription Claims	List			
ListUserSubscriptions	Grants permission to list all User subscriptions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetOverageConfig	Grants permission to set a User subscription overage configuration	Write			
UpdateClaim	Grants permission to update a User subscription Claim	Write			

Resource types defined by AWS User Subscriptions

AWS User Subscriptions does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS User Subscriptions, specify `"Resource": "*"` in your policy.

Condition keys for AWS User Subscriptions

AWS User Subscriptions defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
user-subscriptions:CreateForSelf	Filters access by only allowing creation of User subscription Claims for the caller	Bool

Actions, resources, and condition keys for AWS Verified Access

AWS Verified Access (service prefix: `verified-access`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Verified Access

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVerifiedAccess [permission only]	Grants permission to create Verified Access Instance	Write			

Resource types defined by AWS Verified Access

AWS Verified Access does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Verified Access, specify `"Resource": "*"` in your policy.

Condition keys for AWS Verified Access

Verified Access has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon Verified Permissions

Amazon Verified Permissions (service prefix: `verifiedpermissions`) 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 Verified Permissions
- Resource types defined by Amazon Verified Permissions
- Condition keys for Amazon Verified Permissions

Actions defined by Amazon Verified 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIdentitySource	Grants permission to create a reference to an external identity provider (IdP) that is compatible with OpenID Connect (OIDC) authentic	Write	policy-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	ation protocol, such as Amazon Cognito				
CreatePolicy	Grants permission to create a Cedar policy and save it in the specified policy store	Write	policy-store*		
CreatePolicyStore	Grants permission to create a Cedar policy and save it in the specified policy store	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyTemplate	Grants permission to create a policy template	Write	policy-store*		
DeleteIdentitySource	Grants permission to delete an identity source that references an identity provider (IdP) such as Amazon Cognito	Write	policy-store*		
DeletePolicy	Grants permission to delete the specified policy from the policy store	Write	policy-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicyStore	Grants permission to delete the specified policy store	Write	policy-store*		
DeletePolicyTemplate	Grants permission to delete the specified policy template from the policy store	Write	policy-store*		
GetIdentitySource	Grants permission to retrieve the details about the specified identity source	Read	policy-store*		
GetPolicy	Grants permission to retrieve information about the specified policy	Read	policy-store*		
GetPolicyStore	Grants permission to retrieve details about a policy store	Read	policy-store*		verifiedpermissions:ListTagsForResource
GetPolicyTemplate	Grants permission to retrieve the details for the specified policy template in the specified policy store	Read	policy-store*		
GetSchema	Grants permission to retrieve the details for the specified schema in the specified policy store	Read	policy-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
IsAuthorized	Grants permission to make an authorization decision about a service request described in the parameters	Read	policy-store*		
IsAuthorizedWithToken	Grants permission to make an authorization decision about a service request described in the parameters. The principal in this request comes from an external identity source	Read	policy-store*		
ListIdentitySources	Grants permission to return a paginated list of all of the identity sources defined in the specified policy store	List	policy-store*		
ListPolicies	Grants permission to return a paginated list of all policies stored in the specified policy store	List	policy-store*		
ListPolicyStores	Grants permission to return a paginated list of all policy stores in the calling Amazon Web Services account	List			
ListPolicyTemplates	Grants permission to return a paginated list of all policy templates in the specified policy store	List	policy-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to view a list of resource tags for the specified policy store	Read	policy-store*		
PutSchema	Grants permission to create or update the policy schema in the specified policy store	Write	policy-store*		
TagResource	Grants permission to add tags to the specified policy store	Tagging	policy-store*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from the specified policy store	Tagging	policy-store*		
				aws:TagKeys	
UpdateIdentitySource	Grants permission to update the specified identity source to use a new identity provider (IdP) source, or to change the mapping of identities from the IdP to a different principal entity type	Write	policy-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePolicy	Grants permission to modify the specified Cedar static policy in the specified policy store	Write	policy-store*		
UpdatePolicyStore	Grants permission to modify the validation setting for a policy store	Write	policy-store*		
UpdatePolicyTemplate	Grants permission to update the specified policy template	Write	policy-store*		

Resource types defined by Amazon Verified Permissions

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-store	`arn:${Partition}:verifiedpermissions::${Account}:policy-store/${PolicyStoreId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Verified Permissions

Amazon Verified Permissions defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon VPC Lattice

Amazon VPC Lattice (service prefix: `vpc-lattice`) 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 VPC Lattice
- Resource types defined by Amazon VPC Lattice
- Condition keys for Amazon VPC Lattice

Actions defined by Amazon VPC Lattice

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateViaAWSService [permission only]	Grants permission to associate a resource configuration through any AWS service managed networks	Permissions management			
AssociateViaAWSService-EventsAndStates [permission only]	Grants permission to associate a resource configuration through Amazon EventBridge and AWS Step Functions service networks	Permissions management			
CreateAccessLogSubscription	Grants permission to create an access log subscription	Write	AccessLogSubscription*		logs:CreateLogDelivery logs:GetLogDelivery
			ResourceConfiguration		
			Service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ServiceNetwork		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction	
CreateListener	Grants permission to create a listener	Write	Listener*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:Protocol vpc-lattice:TargetGroupArns vpc-lattice:CreateAction	
CreateResourceConfiguration	Grants permission to create a resource configuration	Write	DomainVerification		
			ResourceConfiguration		
			ResourceGateway		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction	
CreateResourceGateway	Grants permission to create a resource gateway	Write	ResourceGateway*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId vpc-lattice:CreateAction	
CreateRule	Grants permission to create a rule	Write	Rule*		
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:TargetGroupArns vpc-lattice:CreateAction	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateService	Grants permission to create a service	Write	Service*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction	
CreateServiceNetwork	Grants permission to create a service network	Write	ServiceNetwork*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction	
CreateServiceNetworkResourceAssociation	Grants permission to create an association between a service network and a resource	Write	ResourceConfiguration*		
			ServiceNetwork*		
			ServiceNetworkResourceAssociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn vpc-lattice:CreateAction	
CreateServiceNetworkServiceAssociation	Grants permission to create a service network and service association	Write	Service*		
			ServiceNetwork*		
			ServiceNetworkServiceAssociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn vpc-lattice:CreateAction	
CreateServiceNetworkVpcAssociation	Grants permission to create a service network and VPC association	Write	ServiceNetwork* ServiceNetworkVpcAssociation*		ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:PrivateDnsPreference vpc-lattice:PrivateDnsSpecifiedDomains vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				vpc-lattice:CreateAction	
CreateServiceNetworkVpcEndpointAssociation [permission only]	Grants permission to create an association between a service network and VPC endpoint	Permissions management			
CreateTargetGroup	Grants permission to create a target group	Write	TargetGroup*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:VpcId vpc-lattice:CreateAction	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccessLogSubscription	Grants permission to delete an access log subscription	Write	AccessLogSubscription*		logs:DeleteLogDelivery logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	
DeleteAuthPolicy	Grants permission to delete an auth policy	Permissions management	Service		
			ServiceNetwork		
DeleteDomainVerification	Grants permission to delete a domain verification	Write	DomainVerification*		
				aws:ResourceTag/${TagKey}	
DeleteListener	Grants permission to delete a listener	Write	Listener*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourceConfiguration	Grants permission to delete a resource configuration	Write	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
DeleteResourceEndpointAssociation	Grants permission to delete a resource endpoint association	Write	ResourceEndpointAssociation*		
				aws:ResourceTag/${TagKey}	
DeleteResourceGateway	Grants permission to delete a resource gateway	Write	ResourceGateway*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Grants permission to delete a resource policy	Write	ResourceConfiguration		
			Service		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ServiceNetwork		
DeleteRule	Grants permission to delete a rule	Write	Rule*		
				aws:ResourceTag/${TagKey}	
DeleteService	Grants permission to delete a service	Write	Service*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetwork	Grants permission to delete a service network	Write	ServiceNetwork*		
				aws:ResourceTag/${TagKey}	
DeleteServiceNetworkResourceAssociation	Grants permission to delete the association between a service network and resource	Write	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteServiceNetworkServiceAssociation	Grants permission to delete a service network service association	Write	ServiceNetworkServiceAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
DeleteServiceNetworkVpcAssociation	Grants permission to delete a service network and VPC association	Write	ServiceNetworkVpcAssociation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
DeleteTargetGroup	Grants permission to delete a target group	Write	TargetGroup*		
				aws:ResourceTag/${TagKey}	
DeregisterTargets	Grants permission to deregister targets from a target group	Write	TargetGroup*		
GetAccessLogSubscription	Grants permission to get information about an access log subscription	Read	AccessLogSubscription*		logs:GetLogDelivery
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAuthPolicy	Grants permission to get information about an auth policy	Read	Service		
			ServiceNetwork		
GetDomainVerification	Grants permission to get information about a domain verification	Read	DomainVerification*		
				aws:ResourceTag/${TagKey}	
GetListener	Grants permission to get information about a listener	Read	Listener*		
				aws:ResourceTag/${TagKey}	
GetResourceConfiguration	Grants permission to get information about a resource configuration	Read	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
GetResourceGateway	Grants permission to get information about a resource gateway	Read	ResourceGateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetResourcePolicy	Grants permission to get information about a resource policy	Read	ResourceConfiguration		
			Service		
			ServiceNetwork		
GetRule	Grants permission to get information about a rule	Read	Rule*		
				aws:ResourceTag/${TagKey}	
GetService	Grants permission to get information about a service	Read	Service*		
				aws:ResourceTag/${TagKey}	
GetServiceNetwork	Grants permission to get information about a service network	Read	ServiceNetwork*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetServiceNetworkResourceAssociation	Grants permission to get information about an association between a service network and resource configuration	Read	ServiceNetworkResourceAssociation*		
				aws:ResourceTag/${TagKey}	
GetServiceNetworkServiceAssociation	Grants permission to get information about a service network and service association	Read	ServiceNetworkServiceAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServiceNetworkVpcAssociation	Grants permission to get information about a service network and VPC association	Read	ServiceNetworkVpcAssociation*		
				aws:ResourceTag/${TagKey} vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
GetTargetGroup	Grants permission to get information about a target group	Read	TargetGroup*		
				aws:ResourceTag/${TagKey}	
ListAccessLogSubscriptions	Grants permission to list some or all access log subscriptions about a service network or a service	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDomainVerifications	Grants permission to list some or all domain verifications	List			
ListListeners	Grants permission to list some or all listeners	List			
ListResourceConfigurations	Grants permission to list some or all resource configurations	List			
ListResourceEndpointAssociations	Grants permission to list some or all associations between a resource configuration and VPC endpoint	List		vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId	
ListResourceGateways	Grants permission to list some or all resource gateways	List			
ListRules	Grants permission to list some or all rules	List			
ListServiceNetworkResourceAssociations	Grants permission to list some or all associations between a service network and resource configuration	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServiceNetworkServiceAssociations	Grants permission to list some or all service network and service associations	List		vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn	
ListServiceNetworkVpcAssociations	Grants permission to list some or all service network and VPC associations	List		vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
ListServiceNetworkVpcEndpointAssociations	Grants permission to list some or all associations between a service network and VPC endpoint	List			
ListServiceNetworks	Grants permission to list the service networks owned by a caller account or shared with the caller account	List			
ListServices	Grants permission to list the services owned by a caller account or shared with the caller account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a vpc-lattice resource	Read			
ListTargetGroups	Grants permission to list some or all target groups	List			
ListTargets	Grants permission to list some or all targets in a target group	List	TargetGroup*		
PutAuthPolicy	Grants permission to create or update the auth policy for a service network or a service	Permissions management	Service		
			ServiceNetwork		
PutResourcePolicy	Grants permission to create a resource policy for a resource configuration, service, or service network	Write	ResourceConfiguration		
			Service		
			ServiceNetwork		
RegisterTargets	Grants permission to register targets to a target group	Write	TargetGroup*		
StartDomainVerification	Grants permission to start a domain verification	Write	DomainVerification*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys vpc-lattice:DomainName vpc-lattice:CreateAction	
TagResource	Grants permission to tag a vpc-lattice resource	Tagging	AccessLogSubscription		
			DomainVerification		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ResourceGateway		
			Rule		
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		

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 vpc-lattice resource	Tagging	AccessLogSubscription		
			DomainVerification		
			Listener		
			ResourceConfiguration		
			ResourceEndpointAssociation		
			ResourceGateway		
			Rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Service		
			ServiceNetwork		
			ServiceNetworkResourceAssociation		
			ServiceNetworkServiceAssociation		
			ServiceNetworkVpcAssociation		
			TargetGroup		
				aws:TagKeys	
UpdateAccessLogSubscription	Grants permission to update an access log subscription	Write	AccessLogSubscription*		logs:GetLogDelivery logs:UpdateLogDelivery

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateListener	Grants permission to update a listener	Write	Listener*		
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateResourceConfiguration	Grants permission to update a resource configuration	Write	ResourceConfiguration*		
				aws:ResourceTag/${TagKey}	
UpdateResourceGateway	Grants permission to update a resource gateway	Write	ResourceGateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} vpc-lattice:SecurityGroupIds	
UpdateRule	Grants permission to update a rule	Write	Rule*		
				aws:ResourceTag/${TagKey} vpc-lattice:TargetGroupArns	
UpdateService	Grants permission to update a service	Write	Service*		
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetwork	Grants permission to update a service network	Write	ServiceNetwork*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} vpc-lattice:AuthType	
UpdateServiceNetworkVpcAssociation	Grants permission to update a service network and VPC association	Write	ServiceNetworkVpcAssociation*		ec2:DescribeSecurityGroups ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId	
UpdateTargetGroup	Grants permission to update a target group	Write	TargetGroup*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon VPC Lattice

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
AccessLog Subscription	arn:${Partition}:vpc-lattice:${Region}:${Account}:accesslogsubscription/${AccessLogSubscriptionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction
DomainVerification	arn:${Partition}:vpc-lattice:${Region}:${Account}:domainverification/${DomainVerificationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:DomainName
Listener	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Resource types	ARN	Condition keys
		vpc-lattice:CreateAction vpc-lattice:Protocol vpc-lattice:TargetGroupArns
ResourceConfiguration	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceconfiguration/${ResourceConfigurationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction
ResourceEndpointAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourceendpointassociation/${ResourceEndpointAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:ResourceConfigurationArn vpc-lattice:VpcEndpointId

Resource types	ARN	Condition keys
ResourceGateway	arn:${Partition}:vpc-lattice:${Region}:${Account}:resourcegateway/${ResourceGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:VpcId
Rule	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/listener/${ListenerId}/rule/${RuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:TargetGroupArns

Resource types	ARN	Condition keys
Service	arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction
ServiceNetwork	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetwork/${ServiceNetworkId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:AuthType vpc-lattice:CreateAction

Resource types	ARN	Condition keys
ServiceNetworkResourceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkresourceassociation/${ServiceNetworkResourceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:ResourceConfigurationArn vpc-lattice:ServiceNetworkArn
ServiceNetworkServiceAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkserviceassociation/${ServiceNetworkServiceAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:ServiceArn vpc-lattice:ServiceNetworkArn

Resource types	ARN	Condition keys
ServiceNetworkVpcAssociation	arn:${Partition}:vpc-lattice:${Region}:${Account}:servicenetworkvpcassociation/${ServiceNetworkVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:PrivateDnsPreference vpc-lattice:PrivateDnsSpecifiedDomains vpc-lattice:SecurityGroupIds vpc-lattice:ServiceNetworkArn vpc-lattice:VpcId

Resource types	ARN	Condition keys
TargetGroup	arn:${Partition}:vpc-lattice:${Region}:${Account}:targetgroup/${TargetGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys vpc-lattice:CreateAction vpc-lattice:VpcId

Condition keys for Amazon VPC Lattice

Amazon VPC Lattice defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
vpc-lattice:AuthType	Filters access by the auth type specified in the request	String

Condition keys	Description	Type
vpc-lattice:CreateAction	Filters access by the name of a resource-creating API action	String
vpc-lattice:DomainName	Filters access by the domain name	String
vpc-lattice:PrivateDnsPreference	Filters access by the private dns preference	String
vpc-lattice:PrivateDnsSpecifiedDomains	Filters access by the private dns domains	ArrayOfString
vpc-lattice:Protocol	Filters access by the protocol specified in the request	String
vpc-lattice:ResourceConfigurationArn	Filters access by the ARN of a resource configuration	ARN
vpc-lattice:SecurityGroupIds	Filters access by the IDs of security groups	ArrayOfString
vpc-lattice:ServiceArn	Filters access by the ARN of a service	ARN
vpc-lattice:ServiceNetworkArn	Filters access by the ARN of a service network	ARN
vpc-lattice:TargetGroupArns	Filters access by the ARNs of target groups	ArrayOfARN

Condition keys	Description	Type
vpc-lattice:VpcEndpointId	Filters access by the ID of a VPC endpoint	String
vpc-lattice:VpcId	Filters access by the ID of a virtual private cloud (VPC)	String

Actions, resources, and condition keys for Amazon VPC Lattice Services

Amazon VPC Lattice Services (service prefix: `vpc-lattice-svcs`) 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 VPC Lattice Services
- Resource types defined by Amazon VPC Lattice Services
- Condition keys for Amazon VPC Lattice Services

Actions defined by Amazon VPC Lattice Services

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Connect	Grants permission to connect to a VPC Lattice service	Write	TCP Service*		
				vpc-lattice-svcs:Port vpc-lattice-svcs:ServiceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount	
Invoke	Grants permission to invoke a VPC Lattice service	Write	Service*		
				vpc-lattice-svcs:Port vpc-lattice-svcs:S	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				erviceNetworkArn vpc-lattice-svcs:ServiceArn vpc-lattice-svcs:SourceVpc vpc-lattice-svcs:SourceVpcOwnerAccount vpc-lattice-svcs:RequestMethod vpc-lattice-svcs:RequestPath vpc-lattice-svcs:RequestHeader/${HeaderName}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	

Resource types defined by Amazon VPC Lattice Services

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
Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}/${RequestPath}`	
TCP Service	`arn:${Partition}:vpc-lattice:${Region}:${Account}:service/${ServiceId}`	

Condition keys for Amazon VPC Lattice Services

Amazon VPC Lattice Services defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
vpc-lattice-svcs:Port	Filters access by the destination port the request is made to	Numeric
vpc-lattice-svcs:RequestHeader/${HeaderName}	Filters access by a header name-value pair in the request headers	String
vpc-lattice-svcs:RequestMethod	Filters access by the method of the request	String
vpc-lattice-svcs:RequestPath	Filters access by the path portion of the request URL	String
vpc-lattice-svcs:RequestQueryString/${QueryStringKey}	Filters access by the query string key-value pairs in the request URL	ArrayOfString
vpc-lattice-svcs:ServiceArn	Filters access by the ARN of the service receiving the request	ARN
vpc-lattice-svcs:ServiceNetworkArn	Filters access by the ARN of the service network receiving the request	ARN
vpc-lattice-svcs:SourceVpc	Filters access by the VPC the request is made from	String

Condition keys	Description	Type
vpc-lattice-svcs:SourceVpcOwnerAccount	Filters access by the owning account of the VPC the request is made from	String

Actions, resources, and condition keys for AWS WAF

AWS WAF (service prefix: `waf`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS WAF
- Resource types defined by AWS WAF
- Condition keys for AWS WAF

Actions defined by AWS WAF

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateByteMatchSet	Grants permission to create a ByteMatchSet	Write	bytematchset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGeoMatchSet	Grants permission to create a GeoMatchSet	Write	geomatchset*		
CreateIPSet	Grants permission to create an IPSet	Write	ipset*		
CreateRateBasedRule	Grants permission to create a RateBasedRule for limiting the volume of requests from a single IP address	Write	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Grants permission to create a RegexMatchSet	Write	regexmatchset*		
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset*		
CreateRule	Grants permission to create a Rule for filtering web requests	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRuleGroup	Grants permission to create a RuleGroup, which is a collection of predefined rules that you can use in a WebACL	Write	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Grants permission to create a SizeConstraintSet	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	Grants permission to create an SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
CreateWebACL	Grants permission to create a WebACL, which contains rules for filtering web requests	Permissions management	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWebACLMigrationStack	Grants permission to create a CloudFormation web ACL template in an S3 bucket for the purposes of migrating the web ACL from AWS WAF Classic to AWS WAF v2	Write	webacl*		s3:PutObject
CreateXssMatchSet	Grants permission to create an XssMatchSet, which you use to detect requests that contain cross-site scripting attacks	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 the 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
GetByteMatchSet	Grants permission to retrieve a ByteMatchSet	Read	bytematchset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 for a web ACL	Read	webacl*		
GetPermissionPolicy	Grants permission to retrieve an IAM policy for a rule group	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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRule	Grants permission to retrieve a Rule	Read	rule*		
GetRuleGroup	Grants permission to retrieve a RuleGroup	Read	rulegroup*		
GetSampledRequests	Grants permission to retrieve detailed information about 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*		
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			
ListRuleGroups	Grants permission to retrieve an array of RuleGroup objects	List			
ListRules	Grants permission to retrieve an array of RuleSummary objects	List			
ListSizeConstraintSets	Grants permission to retrieve an array of SizeConstraintSetSummary objects	List			
ListSqlInjectionMatchSets	Grants permission to retrieve an array of SqlInjectionMatchSet objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSubscribedRuleGroups	Grants permission to retrieve an array of RuleGroup objects that you are subscribed to	List			
ListTagsForResource	Grants permission to retrieve 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 associate a LoggingConfiguration with a specified web ACL	Write	webacl*		iam:CreateServiceLinkedRole
PutPermissionPolicy	Grants permission to attach an IAM policy to a rule group, to share the rule group between accounts	Permissions management	rulegroup*		
TagResource	Grants permission to add a Tag to a resource	Tagging	ratebasedrule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIPSet	Grants permission to insert or delete IPSetDescriptor objects in an IPSet	Write	ipset*		
UpdateRateBasedRule	Grants permission to modify a rate based 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 modify a Rule	Write	rule*		
UpdateRuleGroup	Grants permission to insert or delete ActivatedRule objects in a RuleGroup	Write	rulegroup*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS WAF

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:${Partition}:waf::${Account}:bytematchset/${Id}`	
ipset	`arn:${Partition}:waf::${Account}:ipset/${Id}`	
ratebasedrule	`arn:${Partition}:waf::${Account}:ratebasedrule/${Id}`	aws:ResourceTag/${TagKey}
rule	`arn:${Partition}:waf::${Account}:rule/${Id}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
sizeconstraintset	arn:${Partition}:waf::${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf::${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf::${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf::${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf::${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf::${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf::${Account}:geomatchset/${Id}	
rulegroup	arn:${Partition}:waf::${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS WAF

AWS WAF defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value associated with the resource	String
aws:TagKeys	Filters actions based on the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS WAF Regional

AWS 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 AWS WAF Regional
- Resource types defined by AWS WAF Regional
- Condition keys for AWS WAF Regional

Actions defined by AWS 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Grants permission to create a RuleGroup	Write	rulegroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Grants permission to create a SizeConstraintSet	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	Grants permission to create an SqlInjectionMatchSet	Write	sqlinjectionmatchset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 AWS WAF Classic to AWS WAF v2	Write	webacl*		s3:PutObject
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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/*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 ByteMatch SetSummary objects	List			
ListGeoMatchSets	Grants permission to retrieve an array of GeoMatchS etSummary objects	List			
ListIPSets	Grants permission to retrieve an array of IPSetSummary objects	List			
ListLoggingConfigurations	Grants permission to retrieve an array of LoggingCo nfiguration objects	List			
ListRateBasedRules	Grants permission to retrieve an array of RuleSummary objects	List			
ListRegexMatchSets	Grants permission to retrieve an array of RegexMatc hSetSummary objects	List			
ListRegexPatternSets	Grants permission to retrieve an array of RegexPatt ernSetSummary objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove a Tag from a resource	Tagging	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 AWS 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}`	
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}

Resource types	ARN	Condition keys
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}	
rulegroup	arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS WAF Regional

AWS 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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value assoicated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters actions based on the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS WAF V2

AWS WAF V2 (service prefix: `wafv2`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS WAF V2
- Resource types defined by AWS WAF V2
- Condition keys for AWS WAF V2

Actions defined by AWS WAF V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate WebACL	Grants permission to associate a WebACL with a resource	Write	webacl*		amplify:AssociateWebACL

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					apigateway:SetWebACL apprunner:AssociateWebAcl appsync:AssociateWebACL appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl elasticloadbalancing:CreateWebACLAssociation elasticloadbalanci

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ng:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
CheckCapacity	Grants permission to calculate web ACL capacity unit (WCU) requirements for a specified scope and set of rules	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
CreateRuleGroup	Grants permission to create a RuleGroup	Write	rulegroup*		wafv2:TagResource
			ipset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	Grants permission to create a WebACL	Write	webacl*		wafv2:TagResource
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAPIKey	Grants permission to delete an API key	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:DisassociateWebACL appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:Delete

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					WebACLAssociation elasticloadbalancing:SetWebAcl 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey}	
GetRegexPatternSet	Grants permission to retrieve details about a RegexPatternSet	Read	regexpatternset*		
				aws:ResourceTag/${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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTopPathStatisticsByTraffic	Grants permission to retrieve aggregated path statistics with bot traffic analysis for a WebACL within a specified time window	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 appsync:GetWebACLForResource cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl elasticloadbalancing:GetLoadBalancerWebACL wafv2:GetWebACL

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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 appsync:ListResourcesForWebACL cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations elasticloadbalancing:DescribeWebACLA

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ssociation
			amplify-app		
			apprunner		
			userpool		
			verified-access-instance		
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
				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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to associate tags with a AWS resource	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to disassociate tags from an AWS resource	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIPSet	Grants permission to update an IPSet	Write	ipset*		
				aws:ResourceTag/${TagKey}	
UpdateManagedRuleSetVersionExpiryDate	Grants permission to update the expiry date of a version in ManagedRuleSet	Write	managedruleset*		
UpdateRegexPatternSet	Grants permission to update a RegexPatternSet	Write	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	Grants permission to update a RuleGroup	Write	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWebACL	Grants permission to update a WebACL	Write	webacl*		
			ipset		
			managedruleset		
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS WAF V2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}	aws:ResourceTag/${TagKey}
managedruleset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/managedruleset/${Name}/${Id}	
rulegroup	arn:${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}	

Resource types	ARN	Condition keys
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	
amplify-app	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}	

Condition keys for AWS WAF V2

AWS WAF V2 defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString
wafv2:LogDestinationResource	Filters access by log destination ARN for PutLoggingConfiguration API	ARN
wafv2:LogScope	Filters access by log scope for Logging Configuration API	String

Actions, resources, and condition keys for AWS Well-Architected Tool

AWS Well-Architected Tool (service prefix: `wellarchitected`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS Well-Architected Tool

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Lenses	Grants permission to associate a lens to the specified workload	Write	workload*		
				aws:ResourceTag/${TagKey}	
Associate Profiles	Grants permission to associate a profile to the specified workload	Write	workload*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
Configure Integration [permission only]	Grants permission to configure the integration	Write			
CreateLensShare	Grants permission to an owner of a lens to share with other AWS accounts and IAM users	Write	lens*		
				aws:ResourceTag/${TagKey}	
CreateLensVersion	Grants permission to create a new lens version	Write	lens*		
				aws:ResourceTag/${TagKey}	
CreateMilestone	Grants permission to create a new milestone for the specified workload	Write	workload*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProfile	Grants permission to create a new profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileShare	Grants permission to an owner of a profile to share with other AWS accounts and IAM users	Write	profile*		
				aws:ResourceTag/${TagKey}	
CreateReviewTemplate	Grants permission to create a new review template	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateShare	Grants permission to an owner of a review template to share with other AWS accounts and IAM users	Write	review-template*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkload	Grants permission to create a new workload	Write		aws:RequestTag/${TagKey} aws:TagKeys wellarchitected:JiraProjectKey	
CreateWorkloadShare	Grants permission to share a workload with another account	Write	workload*		
				aws:ResourceTag/${TagKey}	
DeleteLens	Grants permission to delete a lens	Write	lens*		
				aws:ResourceTag/${TagKey}	
DeleteLensShare	Grants permission to delete an existing lens share	Write	lens*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProfile	Grants permission to delete a profile	Write	profile*		
				aws:ResourceTag/${TagKey}	
DeleteProfileShare	Grants permission to delete an existing profile share	Write	profile*		
				aws:ResourceTag/${TagKey}	
DeleteReviewTemplate	Grants permission to delete an existing review template	Write	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteTemplateShare	Grants permission to delete an existing review template share	Write	review-template*		
				aws:ResourceTag/${TagKey}	
DeleteWorkload	Grants permission to delete an existing workload	Write	workload*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteWorkloadShare	Grants permission to delete an existing workload share	Write	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateLenses	Grants permission to disassociate a lens from the specified workload	Write	workload*		
				aws:ResourceTag/${TagKey}	
DisassociateProfiles	Grants permission to disassociate a profile from the specified workload	Write	workload*		
				aws:ResourceTag/${TagKey}	
ExportLens	Grants permission to export an existing lens	Read	lens*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAnswer	Grants permission to retrieve the specified answer from the specified lens review	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetConsolidatedReport	Grants permission to get consolidated report metrics or to generate the consolidated report PDF in this account	Read			
GetGlobalSettings	Grants permission to get all settings for the account	Read			
GetLens	Grants permission to get an existing lens	Read	lens*		
				aws:ResourceTag/${TagKey}	
GetLensReview	Grants permission to retrieve the specified lens review of the specified workload	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetLensReviewReport	Grants permission to retrieve the report for the specified lens review	Read	workload*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetLensVersionDifference	Grants permission to get the difference between the specified lens version and latest available lens version	Read	lens*		
				aws:ResourceTag/${TagKey}	
GetMilestone	Grants permission to retrieve the specified milestone of the specified workload	Read	workload*		
				aws:ResourceTag/${TagKey}	
GetProfile	Grants permission to retrieve the specified profile	Read	profile*		
				aws:ResourceTag/${TagKey}	
GetProfileTemplate	Grants permission to retrieve the specified profile template	Read			
GetReviewTemplate	Grants permission to retrieve the specified review template	Read	review-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetReviewTemplateAnswer	Grants permission to retrieve the specified answer from the specified review template lens review	Read	review-template*		
				aws:ResourceTag/${TagKey}	
GetReviewTemplateLensReview	Grants permission to retrieve the specified lens review of the specified review template	Read	review-template*		
				aws:ResourceTag/${TagKey}	
GetWorkload	Grants permission to retrieve the specified workload	Read	workload*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportLens	Grants permission to import a new lens	Write		aws:RequestTag/${TagKey} aws:TagKeys	
ListAnswers	Grants permission to list the answers from the specified lens review	List	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckDetails	Grants permission to list the check-details for the workload	List	workload*		
				aws:ResourceTag/${TagKey}	
ListCheckSummaries	Grants permission to list the check-summaries for the workload	List	workload*		
				aws:ResourceTag/${TagKey}	
ListLensReviewImprovements	Grants permission to list the improvements of the specified lens review	List	workload*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListLensReviews	Grants permission to list the lens reviews of the specified workload	List	workload*		
				aws:ResourceTag/${TagKey}	
ListLensShares	Grants permission to list all shares created for a lens	List	lens*		
				aws:ResourceTag/${TagKey}	
ListLenses	Grants permission to list the lenses available to this account	List			
ListMilestones	Grants permission to list the milestones of the specified workload	List	workload*		
				aws:ResourceTag/${TagKey}	
ListNotifications	Grants permission to list notifications related to the account or specified resource	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProfileNotifications	Grants permission to list profile notifications related to specified resource	List			
ListProfileShares	Grants permission to list all shares created for a profile	List	profile*		
				aws:ResourceTag/${TagKey}	
ListProfiles	Grants permission to list the profiles available to this account	List			
ListReviewTemplateAnswers	Grants permission to list the answers from the specified review template lens review	List	review-template*		
				aws:ResourceTag/${TagKey}	
ListReviewTemplates	Grants permission to list the review templates available to this account	List			
ListShareInvitations	Grants permission to list the workload share invitations of the specified account or user	List			
ListTagsForResource	Grants permission to list tags for a Well-Architected resource	Read	lens		
			profile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			review-template		
			workload		
				aws:ResourceTag/${TagKey}	
ListTemplateShares	Grants permission to list all shares created for a review template	List	review-template*		
				aws:ResourceTag/${TagKey}	
ListWorkloadShares	Grants permission to list the workload shares of the specified workload	List	workload*		
				aws:ResourceTag/${TagKey}	
ListWorkloads	Grants permission to list the workloads in this account	List			
TagResource	Grants permission to tag a Well-Architected resource	Tagging	lens		
			profile		
			review-template		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workload		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a Well-Architected resource	Tagging	lens		
			profile		
			review-template		
			workload		
				aws:TagKeys	
UpdateAnswer	Grants permission to update properties of the specified answer	Write	workload*		
				aws:ResourceTag/${TagKey}	
UpdateGlobalSettings	Grants permission to manage all settings for the account	Write		wellarchitected:JiraProjectKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIntegration	Grants permission to update properties of the integration	Write	workload*		
				aws:ResourceTag/${TagKey}	
UpdateLensReview	Grants permission to update properties of the specified lens review	Write	workload*		
				aws:ResourceTag/${TagKey}	
UpdateProfile	Grants permission to update properties of the specified profile	Write	profile*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplate	Grants permission to update properties of the specified review template	Write	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateAnswer	Grants permission to update properties of the specified review template answer	Write	review-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateReviewTemplateLensReview	Grants permission to update properties of the specified review template lens review	Write	review-template*		
				aws:ResourceTag/${TagKey}	
UpdateShareInvitation	Grants permission to update status of the specified workload share invitation	Write			
UpdateWorkload	Grants permission to update properties of the specified workload	Write	workload*		
				aws:ResourceTag/${TagKey} wellarchitected:JiraProjectKey	
UpdateWorkloadShare	Grants permission to update properties of the specified workload share	Write	workload*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpgradeLensReview	Grants permission to upgrade the specified lens review to use the latest version of the associated lens	Write	workload*		
				aws:ResourceTag/${TagKey}	
UpgradeProfileVersion	Grants permission to upgrade the specified workload to use the latest version of the associated profile	Write	profile*		
			workload*		
				aws:ResourceTag/${TagKey}	
UpgradeReviewTemplateLensReview	Grants permission to upgrade the specified lens review of the specified review template	Write	review-template*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS Well-Architected Tool

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
workload	`arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}`	aws:ResourceTag/${TagKey}
lens	`arn:${Partition}:wellarchitected:${Region}:${Account}:lens/${ResourceId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:wellarchitected:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
review-template	`arn:${Partition}:wellarchitected:${Region}:${Account}:review-template/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Well-Architected Tool

AWS Well-Architected Tool defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys in the request	ArrayOfString
wellarchitected:JiraProjectKey	Filters access by project key	String

Actions, resources, and condition keys for AWS Wickr

AWS Wickr (service prefix: `wickr`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Wickr
- Resource types defined by AWS Wickr
- Condition keys for AWS Wickr

Actions defined by AWS Wickr

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCreateUser	Grants permission to batch create users in a Wickr network	Write	network*		
BatchDeleteUser	Grants permission to batch delete users from a Wickr network	Write	network*		
BatchLookupUserUname	Grants permission to batch lookup user unames in a Wickr network	Read	network*		
BatchReinviteUser	Grants permission to batch reinvite users in a Wickr network	Write	network*		
BatchResetDevicesForUser	Grants permission to batch reset devices for a user in a Wickr network	Write	network*		
BatchToggleUserSuspendStatus	Grants permission to batch toggle user suspend status in a Wickr network	Write	network*		
CreateAdminSession	Grants permission to create and manage Wickr networks	Write	network*		
CreateBot	Grants permission to create a bot in a Wickr network	Write	network*		
CreateDataRetentionBot	Grants permission to create a data retention bot in a Wickr network	Write	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataRetentionBotChallenge	Grants permission to create a data retention bot challenge in a Wickr network	Write	network*		
CreateNetwork	Grants permission to create a new Wickr network	Write	network*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSecurityGroup	Grants permission to create a security group in a Wickr network	Write	network*		
DeleteBot	Grants permission to delete a bot from a Wickr network	Write	network*		
DeleteDataRetentionBot	Grants permission to delete a data retention bot from a Wickr network	Write	network*		
DeleteNetwork	Grants permission to delete Wickr networks	Write	network*		
DeleteSecurityGroup	Grants permission to delete a security group from a Wickr network	Write	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBot	Grants permission to get bot information in a Wickr network	Read	network*		
GetBotsCount	Grants permission to get bot count for a Wickr network	Read	network*		
GetDataRetentionBot	Grants permission to get data retention bot information in a Wickr network	Read	network*		
GetGuestUserHistoryCount	Grants permission to get guest user history count for a Wickr network	Read	network*		
GetNetwork	Grants permission to get details of a Wickr network	Read	network*		
GetNetworkSettings	Grants permission to get network settings for a Wickr network	Read	network*		
GetOidcInfo	Grants permission to get OIDC information for a Wickr network	Read	network*		
GetSecurityGroup	Grants permission to get security group information in a Wickr network	Read	network*		
GetUser	Grants permission to get information about a user in a Wickr network	Read	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUsersCount	Grants permission to get user count for a Wickr network	Read	network*		
ListBlockedGuestUsers	Grants permission to list blocked guest users in a Wickr network	Read	network*		
ListBots	Grants permission to list bots in a Wickr network	Read	network*		
ListDevicesForUser	Grants permission to list devices for a user in a Wickr network	Read	network*		
ListGuestUsers	Grants permission to list guest users in a Wickr network	Read	network*		
ListNetworks	Grants permission to list Wickr networks	Read			
ListSecurityGroupUsers	Grants permission to list users in a security group in a Wickr network	Read	network*		
ListSecurityGroups	Grants permission to list security groups in a Wickr network	Read	network*		
ListTagsForResource	Grants permission to list the tags applied to a Wickr resource	Read	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListUsers	Grants permission to list users in a Wickr network	Read	network*		
RegisterOidcConfig	Grants permission to register OIDC configuration for a Wickr network	Write	network*		
RegisterOidcConfigTest	Grants permission to test OIDC configuration for a Wickr network	Write	network*		
TagResource	Grants permission to add tags to a specified Wickr resource	Tagging	network*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag the specified tags from the specified Wickr resource	Tagging	network*		
				aws:TagKeys	
UpdateBot	Grants permission to update a bot in a Wickr network	Write	network*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDataRetention	Grants permission to update data retention settings in a Wickr network	Write	network*		
UpdateGuestUser	Grants permission to update guest user status in a Wickr network	Write	network*		
UpdateNetworkDetails	Grants permission to update Wickr network details	Write	network*		
UpdateNetworkSettings	Grants permission to update network settings for a Wickr network	Write	network*		
UpdateSecurityGroup	Grants permission to update a security group in a Wickr network	Write	network*		
UpdateUser	Grants permission to update user information in a Wickr network	Write	network*		

Resource types defined by AWS Wickr

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
network	`arn:${Partition}:wickr:${Region}:${Account}:network/${NetworkId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Wickr

AWS Wickr defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag's key and value in a request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys in a request	ArrayOfString

Actions, resources, and condition keys for Amazon WorkDocs

Amazon WorkDocs (service prefix: `workdocs`) 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 WorkDocs

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortDocumentVersionUpload	Grants permission to abort the upload of the specified document version that was previously initiated by InitiateDocumentVersionUpload	Write			
ActivateUser	Grants permission to activate the specified user. Only active users can access Amazon WorkDocs	Write			
AddNotificationPermissions [permission only]	Grants permission to add principals that are allowed to call notification subscription APIs for a given WorkDocs site	Write			
AddResourcePermissions	Grants permission to create a set of permissions for the specified folder or document	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddUserToGroup [permission only]	Grants permission to add a user to a group	Write			
CheckAlias [permission only]	Grants permission to check an alias	Read			
CreateComment	Grants permission to add a new comment to the specified document version	Write			
CreateCustomMetadata	Grants permission to add one or more custom properties to the specified resource	Write			
CreateFolder	Grants permission to create a folder with the specified name and parent folder	Write			
CreateInstance [permission only]	Grants permission to create an instance	Write			
CreateLabels	Grants permission to add labels to the given resource	Write			
CreateNotificationSubscription	Grants permission to configure WorkDocs to use Amazon SNS notifications	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser	Grants permission to create a user in a Simple AD or Microsoft AD directory	Write			
DeactivateUser	Grants permission to deactivate the specified user, which revokes the user's access to Amazon WorkDocs	Write			
DeleteComment	Grants permission to delete the specified comment from the document version	Write			
DeleteCustomMetadata	Grants permission to delete custom metadata from the specified resource	Write			
DeleteDocument	Grants permission to permanently delete the specified document and its associated metadata	Write			
DeleteDocumentVersion	Grants permission to delete versions of a specified document	Write			
DeleteFolder	Grants permission to permanently delete the specified folder and its contents	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFolderContents	Grants permission to delete the contents of the specified folder	Write			
DeleteInstance [permission only]	Grants permission to delete an instance	Write			
DeleteLabels	Grants permission to delete one or more labels from a resource	Write			
DeleteNotificationPermissions [permission only]	Grants permission to delete principals that are allowed to call notification subscription APIs for a given WorkDocs site	Write			
DeleteNotificationSubscription	Grants permission to delete the specified subscription from the specified organization	Write			
DeleteUser	Grants permission to delete the specified user from a Simple AD or Microsoft AD directory	Write			
DeregisterDirectory [permission only]	Grants permission to deregister a directory	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeActivities	Grants permission to fetch user activities in a specified time period	List			
DescribeAvailableDirectories [permission only]	Grants permission to describe available directories	List			
DescribeComments	Grants permission to list all the comments for the specified document version	List			
DescribeDocumentVersions	Grants permission to retrieve the document versions for the specified document	List			
DescribeFolderContents	Grants permission to describe the contents of the specified folder, including its documents and sub-folders	List			
DescribeGroups	Grants permission to describe the user groups	List			
DescribeInstanceExports [permission only]	Grants permission to describe the export history for an instance	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstances [permission only]	Grants permission to describe instances	List			
DescribeNotificationPermissions [permission only]	Grants permission to describe principals that are allowed to call notification subscription APIs for a given WorkDocs site	List			
DescribeNotificationSubscriptions	Grants permission to list the specified notification subscriptions	List			
DescribeResourcePermissions	Grants permission to view a description of a specified resource's permissions	List			
DescribeRootFolders	Grants permission to describe the root folders	List			
DescribeUsers	Grants permission to view a description of the specified users. You can describe all users or filter the results (for example, by status or organization)	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DownloadDocumentVersion [permission only]	Grants permission to download a specified document version	Read			
GetCurrentUser	Grants permission to retrieve the details of the current user	Read			
GetDocument	Grants permission to retrieve the specified document object	Read			
GetDocumentPath	Grants permission to retrieve the path information (the hierarchy from the root folder) for the requested document	Read			
GetDocumentVersion	Grants permission to retrieve version metadata for the specified document	Read			
GetFolder	Grants permission to retrieve the metadata of the specified folder	Read			
GetFolderPath	Grants permission to retrieve the path information (the hierarchy from the root folder) for the specified folder	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroup [permission only]	Grants permission to retrieve details for the specified group	Read			
GetResources	Grants permission to get a collection of resources	Read			
InitiateDocumentVersionUpload	Grants permission to create a new document object and version object	Write			
RegisterDirectory [permission only]	Grants permission to register a directory	Write			
RemoveAllResourcePermissions	Grants permission to remove all the permissions from the specified resource	Write			
RemoveResourcePermission	Grants permission to remove the permission for the specified principal from the specified resource	Write			
RestoreDocumentVersions	Grants permission to restore versions of a specified document	Write			
SearchResources	Grants permission to search metadata and the content of resources	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInstanceExport [permission only]	Grants permission to start an export for an instance	Write	organization*		
UpdateDocument	Grants permission to update the specified attributes of the specified document	Write			
UpdateDocumentVersion	Grants permission to change the status of the document version to ACTIVE	Write			
UpdateFolder	Grants permission to update the specified attributes of the specified folder	Write			
UpdateInstanceAlias [permission only]	Grants permission to update an instance alias	Write			
UpdateUser	Grants permission to update the specified attributes of the specified user, and grants or revokes administrative privileges to the Amazon WorkDocs site	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUserAdministrativeSettings [permission only]	Grants permission to update the administrative settings for a user	Write			

Resource types defined by Amazon WorkDocs

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
organization	`arn:${Partition}:workdocs:${Region}:${Account}:organization/${ResourceId}`	

Condition keys for Amazon WorkDocs

WorkDocs has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon WorkLink

Amazon WorkLink (service prefix: `worklink`) 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 WorkLink

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Domain	Grants permission to associate a domain with an Amazon WorkLink fleet	Write	fleet*		
Associate WebsiteAuthorizationProvider	Grants permission to associate a website authorization provider with an Amazon WorkLink fleet	Write	fleet*		
Associate WebsiteCe	Grants permission to associate a website certifica	Write	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
rtificate Authority	te authority with an Amazon WorkLink fleet				
CreateFleet	Grants permission to create an Amazon WorkLink fleet	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFleet	Grants permission to delete an Amazon WorkLink fleet	Write	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeAuditStreamConfiguration	Grants permission to describe the audit stream configuration for an Amazon WorkLink fleet	Read	fleet*		
DescribeCompanyNetworkConfiguration	Grants permission to describe the company network configuration for an Amazon WorkLink fleet	Read	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDevice	Grants permission to describe details of a device associated with an Amazon WorkLink fleet	Read	fleet*		
DescribeDevicePolicyConfiguration	Grants permission to describe the device policy configuration for an Amazon WorkLink fleet	Read	fleet*		
DescribeDomain	Grants permission to describe details about a domain associated with an Amazon WorkLink fleet	Read	fleet*		
DescribeFleetMetadata	Grants permission to describe metadata of an Amazon WorkLink fleet	Read	fleet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIdentityProviderConfiguration	Grants permission to describe the identity provider configuration for an Amazon WorkLink fleet	Read	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWebsiteCertificateAuthority	Grants permission to describe a website certificate authority associated with an Amazon WorkLink fleet	Read	fleet*		
DisassociateDomain	Grants permission to disassociate a domain from an Amazon WorkLink fleet	Write	fleet*		
DisassociateWebsiteAuthorizationProvider	Grants permission to disassociate a website authorization provider from an Amazon WorkLink fleet	Write	fleet*		
DisassociateWebsiteCertificateAuthority	Grants permission to disassociate a website certificate authority from an Amazon WorkLink fleet	Write	fleet*		
ListDevices	Grants permission to list the devices associated with an Amazon WorkLink fleet	List	fleet*		
ListDomains	Grants permission to list the associated domains for an Amazon WorkLink fleet	List	fleet*		
ListFleets	Grants permission to list the Amazon WorkLink fleets associated with the account	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWebsiteAuthorizationProviders	Grants permission to list the website authorization providers for an Amazon WorkLink fleet	List	fleet*		
ListWebsiteCertificateAuthorities	Grants permission to list the website certificate authorities associated with an Amazon WorkLink fleet	List	fleet*		
RestoreDomainAccess	Grants permission to restore access to a domain associated with an Amazon WorkLink fleet	Write	fleet*		
RevokeDomainAccess	Grants permission to revoke access to a domain associated with an Amazon WorkLink fleet	Write	fleet*		
SearchEntity [permission only]	Grants permission to list devices for an Amazon WorkLink fleet	List	fleet*		
SignOutUser	Grants permission to sign out a user from an Amazon WorkLink fleet	Write	fleet*		
TagResource	Grants permission to add one or more tags to a resource	Tagging	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	fleet*		
				aws:TagKeys	
UpdateAuditStreamConfiguration	Grants permission to update the audit stream configuration for an Amazon WorkLink fleet	Write	fleet*		
UpdateCompanyNetworkConfiguration	Grants permission to update the company network configuration for an Amazon WorkLink fleet	Write	fleet*		
UpdateDevicePolicyConfiguration	Grants permission to update the device policy configuration for an Amazon WorkLink fleet	Write	fleet*		
UpdateDomainMetadata	Grants permission to update the metadata for a domain associated with an Amazon WorkLink fleet	Write	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFleetMetadata	Grants permission to update the metadata of an Amazon WorkLink fleet	Write	fleet*		
UpdateIdentityProviderConfiguration	Grants permission to update the identity provider configuration for an Amazon WorkLink fleet	Write	fleet*		

Resource types defined by Amazon WorkLink

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
fleet	`arn:${Partition}:worklink::${Account}:fleet/${FleetName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon WorkLink

Amazon WorkLink defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${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 WorkMail

Amazon WorkMail (service prefix: `workmail`) 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 WorkMail
- Resource types defined by Amazon WorkMail
- Condition keys for Amazon WorkMail

Actions defined by Amazon WorkMail

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for WorkMail audit logs	Write	organization*		
AssociateDelegateToResource	Grants permission to add a member (user or group) to the resource's set of delegates	Write	organization*		
AssociateMemberToGroup	Grants permission to add a member (user or group) to the group's set	Write	organization*		
AssumeImpersonationRole	Grants permission to assume an impersonation role for the given Amazon WorkMail organization	Write	organization*		
				workmail:ImpersonationRoleId	
CancelMailboxExportJob	Grants permission to cancel a currently running mailbox export job	Write	organization*		
CreateAlias	Grants permission to add an alias to the set of a given member (user or group) of WorkMail	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAvailabilityConfiguration	Grants permission to create an AvailabilityConfiguration for the given Amazon WorkMail organization and domain	Write	organization*		
CreateGroup	Grants permission to create a group that can be used in WorkMail by calling the RegisterToWorkMail operation	Write	organization*		
CreateIdentityCenterApplication	Grants permission to create an Identity Center application for WorkMail	Write			
CreateImpersonationRole	Grants permission to create an impersonation role for the given Amazon WorkMail organization	Write	organization*		
CreateInboundMailFlowRule [permission only]	Grants permission to create an inbound email flow rule which will apply to all email sent to an organization	Write	organization*		
CreateMailDomain [permission only]	Grants permission to create a mail domain	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMobileDeviceAccessRule	Grants permission to create a new mobile device access rule	Write	organization*		
CreateOrganization	Grants permission to create a new Amazon WorkMail organization	Write			
CreateOutboundMailFlowRule [permission only]	Grants permission to create an outbound email flow rule which will apply to all email sent from an organization	Write	organization*		
CreateResource	Grants permission to create a new WorkMail resource	Write	organization*		
CreateSmtpGateway [permission only]	Grants permission to register an SMTP gateway to a WorkMail organization	Write	organization*		
CreateUser	Grants permission to create a user, which can be enabled afterwards by calling the RegisterToWorkMail operation	Write	organization*		
DeleteAccessControlRule	Grants permission to delete an access control rule	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAlias	Grants permission to remove one or more specified aliases from a set of aliases for a given user	Write	organization*		
DeleteAvailabilityConfiguration	Grants permission to delete the AvailabilityConfiguration for the given Amazon WorkMail organization and domain	Write	organization*		
DeleteEmailMonitoringConfiguration	Grants permission to delete the email monitoring configuration for an organization	Write	organization*		
DeleteGroup	Grants permission to delete a group from WorkMail	Write	organization*		
DeleteIdentityCenterApplication	Grants permission to delete an Identity Center application for WorkMail	Write			
DeleteIdentityProviderConfiguration	Grants permission to delete the identity provider configuration for the organization	Write	organization*		
DeleteImpersonationRole	Grants permission to delete an impersonation role for the given Amazon WorkMail organization	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInboundMailFlowRule [permission only]	Grants permission to remove an inbound email flow rule to no longer apply to emails sent to an organization	Write	organization*		
DeleteMailDomain [permission only]	Grants permission to remove an unused mail domain from an organization	Write	organization*		
DeleteMailboxPermissions	Grants permission to delete permissions granted to a member (user or group)	Write	organization*		
DeleteMobileDevice [permission only]	Grants permission to remove a mobile device from a user	Write	organization*		
DeleteMobileDeviceAccessOverride	Grants permission to delete a mobile device access override	Write	organization*		
DeleteMobileDeviceAccessRule	Grants permission to delete a mobile device access rule	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOrganization	Grants permission to delete an Amazon WorkMail organization and all underlying AWS resources managed by Amazon WorkMail as part of the organization	Write	organization*		
DeleteOutboundMailFlowRule [permission only]	Grants permission to remove an outbound email flow rule so that it no longer applies to emails sent from an organization	Write	organization*		
DeletePersonalAccessToken	Grants permission to delete a personal access token	Write	organization*		
DeleteResource	Grants permission to delete the specified resource	Write	organization*		
DeleteRetentionPolicy	Grants permission to delete the retention policy based on the supplied organization and policy identifiers	Write	organization*		
DeleteSmtpGateway [permission only]	Grants permission to remove an SMTP gateway from an organization	Write	organization*		
DeleteUser	Grants permission to delete a user from WorkMail and all subsequent systems	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeliverToMailbox [permission only]	Grants permission to deliver emails to a WorkMail organization via the SES MailManager DeliverToMailbox action	Write	organization*		
DeregisterFromWorkMail	Grants permission to mark a user, group, or resource as no longer used in WorkMail	Write	organization*		
DeregisterMailDomain	Grants permission to deregister a mail domain from an organization	Write	organization*		
DescribeEmailMonitoringConfiguration	Grants permission to retrieve the email monitoring configuration for an organization	Read	organization*		
DescribeEntity	Grants permission to read details of an entity	Read	organization*		
DescribeGroup	Grants permission to read the details for a group	List	organization*		
DescribeIdentityProviderConfiguration	Grants permission to read the identity provider configuration for the organization	Read	organization*		
DescribeInboundDmarcSettings	Grants permission to read the settings in a DMARC policy for a specified organization	Read	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInboundMailFlowRule [permission only]	Grants permission to read the details of an inbound mail flow rule configured for an organization	Read	organization*		
DescribeMailDomains [permission only]	Grants permission to show the details of all mail domains associated with the organization	List	organization*		
DescribeMailboxExportJob	Grants permission to retrieve details of a mailbox export job	Read	organization*		
DescribeOrganization	Grants permission to read details of an organization	List	organization*		
DescribeOutboundMailFlowRule [permission only]	Grants permission to read the details of an outbound mail flow rule configured for an organization	Read	organization*		
DescribeResource	Grants permission to read the details for a resource	List	organization*		
DescribeSmtpGateway [permission only]	Grants permission to read the details of an SMTP gateway registered to an organization	Read	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeUser	Grants permission to read details for a user	List	organization*		
DisassociateDelegateFromResource	Grants permission to remove a member from the resource's set of delegates	Write	organization*		
DisassociateMemberFromGroup	Grants permission to remove a member from a group	Write	organization*		
EnableMailDomain [permission only]	Grants permission to enable a mail domain in the organization	Write	organization*		
GetAccessControlEffect	Grants permission to get the effects of access control rules as they apply to a specified IPv4 address, access protocol action, or user ID	Read	organization*		
GetDefaultRetentionPolicy	Grants permission to retrieve the retention policy associated at an organizational level	Read	organization*		
GetImpersonationRole	Grants permission to retrieve an impersonation role for the given Amazon WorkMail organization	Read	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetImpersonationRoleEffect	Grants permission to get the effect of the rules associated to an impersonation role for a specific user	Read	organization*		
GetJournalingRules [permission only]	Grants permission to read the configured journaling and fallback email addresses for email journaling	Read	organization*		
GetMailDomain	Grants permission to retrieve details of a given mail domain in an organization	Read	organization*		
GetMailDomainDetails [permission only]	Grants permission to get the details of the mail domain	Read	organization*		
GetMailboxDetails	Grants permission to read the details of the user's mailbox	Read	organization*		
GetMobileDeviceAccessEffect	Grants permission to simulate the effect of the mobile device access rules for the given attributes of a sample access event	Read	organization*		
GetMobileDeviceAccessOverride	Grants permission to retrieve a mobile device access override	Read	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMobileDeviceDetails [permission only]	Grants permission to get the details of the mobile device	Read	organization*		
GetMobileDevicesForUser [permission only]	Grants permission to get a list of the mobile devices associated with the user	Read	organization*		
GetMobilePolicyDetails [permission only]	Grants permission to get the details of the mobile device policy associated with the organization	Read	organization*		
GetPersonalAccessTokenMetadata	Grants permission to read metadata for a personal access token	Read	organization*		
ListAccessControlRules	Grants permission to list the access control rules	Read	organization*		
ListAliases	Grants permission to list the aliases associated with a given entity	List	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAvailabilityConfigurations	Grants permission to list all the AvailabilityConfiguration's for the given Amazon WorkMail organization	Read	organization*		
ListGroupMembers	Grants permission to read an overview of the members of a group. Users and groups can be members of a group	List	organization*		
ListGroups	Grants permission to list summaries of the organization's groups	List	organization*		
ListGroupsForEntity	Grants permission to list the groups to which an entity belongs	List	organization*		
ListImpersonationRoles	Grants permission to list the impersonation roles for the given Amazon WorkMail organization	List	organization*		
ListInboundMailFlowRules [permission only]	Grants permission to list inbound mail flow rules configured for an organization	List	organization*		
ListMailDomains	Grants permission to list the mail domains for a given organization	List	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMailboxExportJobs	Grants permission to list mailbox export jobs	List	organization*		
ListMailboxPermissions	Grants permission to list the mailbox permissions associated with a user, group, or resource mailbox	List	organization*		
ListMobileDeviceAccessOverrides	Grants permission to list the mobile device access overrides	Read	organization*		
ListMobileDeviceAccessRules	Grants permission to list the mobile device access rules	Read	organization*		
ListOrganizations	Grants permission to list the non-deleted organizations	List			
ListOutboundMailFlowRules [permission only]	Grants permission to list outbound mail flow rules configured for an organization	List	organization*		
ListPersonalAccessTokens	Grants permission to list metadata for personal access tokens	List	organization*		
ListResourceDelegates	Grants permission to list the delegates associated with a resource	List	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResources	Grants permission to list the organization's resources	List	organization*		
ListSmtpGateways [permission only]	Grants permission to list SMTP gateways registered to the organization	List	organization*		
ListTagsForResource	Grants permission to list the tags applied to an Amazon WorkMail organization resource	List	organization*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ListUsers	Grants permission to list the organization's users	List	organization*		
PutAccessControlRule	Grants permission to add a new access control rule	Write	organization*		
PutEmailMonitoringConfiguration	Grants permission to add or update the email monitoring configuration for an organization	Write	organization*		
PutIdentityProviderConfiguration	Grants permission to add or update the identity provider configuration for the organization	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutInboundDmarcSettings	Grants permission to enable or disable a DMARC policy for a given organization	Write	organization*		
PutMailboxPermissions	Grants permission to set permissions for a user, group, or resource, replacing any existing permissions	Write	organization*		
PutMobileDeviceAccessOverride	Grants permission to add or update a mobile device access override	Write	organization*		
PutRetentionPolicy	Grants permission to add or update the retention policy	Write	organization*		
RegisterMailDomain	Grants permission to register a new mail domain in an organization	Write	organization*		
RegisterToWorkMail	Grants permission to register an existing and disabled user, group, or resource for use by associating a mailbox and calendaring capabilities	Write	organization*		
ResetPassword	Grants permission to allow the administrator to reset the password for a user	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchMembers [permission only]	Grants permission to perform a prefix search to find a specific user in a mail group	Read	organization*		
SetDefaultMailDomain [permission only]	Grants permission to set the default mail domain for the organization	Write	organization*		
SetJournalingRules [permission only]	Grants permission to set journaling and fallback email addresses for email journaling	Write	organization*		
SetMobilePolicyDetails [permission only]	Grants permission to set the details of a mobile policy associated with the organization	Write	organization*		
StartMailboxExportJob	Grants permission to start a new mailbox export job	Write	organization*		
TagResource	Grants permission to tag the specified Amazon WorkMail organization resource	Tagging	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TestAvailabilityConfiguration	Grants permission to performs a test on an availability provider to ensure that access is allowed	Read	organization*		
TestInboundMailFlowRules [permission only]	Grants permission to test what inbound rules will apply to an email with a given sender and recipient	Write	organization*		
TestOutboundMailFlowRules [permission only]	Grants permission to test what outbound rules will apply to an email with a given sender and recipient	Write	organization*		
UntagResource	Grants permission to untag the specified Amazon WorkMail organization resource	Tagging	organization*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAvailabilityConfiguration	Grants permission to update an existing AvailabilityConfiguration for the given Amazon WorkMail organization and domain	Write	organization*		
UpdateDefaultMailDomain	Grants permission to update which domain is the default domain for an organization	Write	organization*		
UpdateGroup	Grants permission to update details of a group	Write	organization*		
UpdateImpersonationRole	Grants permission to update an existing impersonation role for the given Amazon WorkMail organization	Write	organization*		
UpdateInboundMailFlowRule [permission only]	Grants permission to update the details of an inbound email flow rule which will apply to all email sent to an organization	Write	organization*		
UpdateMailboxQuota	Grants permission to update the maximum size (in MB) of the user's mailbox	Write	organization*		
UpdateMobileDeviceAccessRule	Grants permission to update a mobile device access rule	Write	organization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOutboundMailFlowRule [permission only]	Grants permission to update the details of an outbound email flow rule which will apply to all email sent from an organization	Write	organization*		
UpdatePrimaryEmailAddress	Grants permission to update the primary email for a user, group, or resource	Write	organization*		
UpdateResource	Grants permission to update details for the resource	Write	organization*		
UpdateSmtpGateway [permission only]	Grants permission to update the details of an existing SMTP gateway registered to an organization	Write	organization*		
UpdateUser	Grants permission to update details of a user	Write	organization*		
WipeMobileDevice [permission only]	Grants permission to remotely wipe the mobile device associated with a user's account	Write	organization*		

Resource types defined by Amazon WorkMail

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
organization	`arn:${Partition}:workmail:${Region}:${Account}:organization/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon WorkMail

Amazon WorkMail defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs that are passed in the request	String
aws:ResourceTag/${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
workmail:ImpersonationRoleId	Filters access by the ImpersonationRoleId that is passed in the request	String

Actions, resources, and condition keys for Amazon WorkMail Message Flow

Amazon WorkMail Message Flow (service prefix: `workmailmessageflow`) 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 WorkMail Message Flow

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRawMessageContent	Grants permission to read the content of email messages with the specified message ID	Read	RawMessage*		
PutRawMessageContent	Grants permission to update the content of email messages with the specified message ID	Write	RawMessage*		

Resource types defined by Amazon WorkMail Message Flow

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
RawMessage	`arn:${Partition}:workmailmessageflow:${Region}:${Account}:message/${OrganizationId}/${Context}/${MessageId}`	

Condition keys for Amazon WorkMail Message Flow

WorkMail Message Flow has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon 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 AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAccountLinkInvitation	Grants permission to accept invitations from other AWS 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 AWS 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	
CreateRootClientCertificate [permission only]	Grants permission to create a root client certificate	Write	certificateid*		
CreateStandbyWorkspaces	Grants permission to create one or more Standby WorkSpaces	Write	directoryid* workspaceid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Grants permission to create tags for WorkSpaces resources	Tagging		aws:RequestTag/${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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceImage	Grants permission to create a new WorkSpace image	Write	workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaces	Grants permission to create one or more WorkSpaces	Write	directoryid*	aws:ResourceTag/${TagKey}	
			workspacebundle*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workspaceid*	aws:RequestTag/${TagKey} aws:TagKeys	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspacesPool	Grants permission to create a WorkSpaces Pool	Write	directoryid*		
			workspacebundle*		
			workspacespoolid*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccountLinkInvitation	Grants permission to delete invitations to other AWS accounts to share the same configuration for WorkSpaces BYOL	Write			
DeleteClientBranding	Grants permission to delete AWS WorkSpaces Client branding data within a directory	Write	directoryid*		
DeleteConnectClientAddIn	Grants permission to delete an Amazon Connect client add-in that is configured within a directory	Write	directoryid*		
DeleteConnectionAlias	Grants permission to delete connection aliases	Write	connectionalias*		
DeleteIpGroup	Grants permission to delete IP access control groups	Write	workspaceipgroup*		
DeleteRootClientCertificate [permission only]	Grants permission to delete root client certificate	Write	certificateid*		

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 AWS 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 AWS accounts for connection aliases	Read	connectionalias*		
DescribeConnectionAliases	Grants permission to retrieve a list that describes the connection aliases used for cross-Region redirection	Read			
DescribeConsent [permission only]	Grants permission to retrieve information about consent agreement to BYOL minimum requirements	Read			
DescribeCustomWorkspaceImageImport	Grants permission to retrieve information about WorkSpace BYOL image import task	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageAssociations	Grants permission to retrieve information about resources associated with a WorkSpace image	List	workspaceimage*		
				aws:ResourceTag/${TagKey}	
DescribeIpGroups	Grants permission to retrieve information about IP access control groups	Read	workspaceipgroup*		
DescribeTags	Grants permission to describe the tags for WorkSpaces resources	Read			
DescribeWorkspaceAssociations	Grants permission to retrieve information about resources associated with a WorkSpace	List	workspaceid*		
				aws:ResourceTag/${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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DirectoryAccessManagement [permission only]	Grants permission to directory management actions while managing and provisioning workspaces	List	directoryid*		
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*		
				aws:ResourceTag/${TagKey}	
GetAccountLink	Grants permission to retrieve a link with another AWS Account for sharing configuration for WorkSpaces BYOL	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportClientBranding	Grants permission to import AWS WorkSpaces Client branding data within a directory	Write	directory id*		
ImportCustomWorkspaceImage	Grants permission to import Bring Your Own License (BYOL) images into Amazon WorkSpaces	Write			
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 AWS 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			
MigrateWorkspace	Grants permission to migrate WorkSpaces	Write	workspacebundle* workspaceid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	directory id*		
ModifyClientProperties	Grants permission to modify the properties of WorkSpaces clients	Write	directory id*		
ModifyEndpointEncryptionMode	Grants permission to configure the specified directory between Standard TLS and FIPS 140-2 validated mode	Write	directory id*		
ModifySamlProperties	Grants permission to modify the SAML properties of a directory	Write	directory id*		
ModifySelfservicePermissions	Grants permission to modify the self-service WorkSpace management capabilities for your users	Permissions management	directory id*		
ModifyStreamingProperties	Grants permission to modify the streaming properties	Write	directory id*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyWorkspaceAccessProperties	Grants permission to specify which devices and operating systems users can use to access their WorkSpaces	Write	directory id*		
ModifyWorkspaceCreationProperties	Grants permission to modify the default properties used to create WorkSpaces	Write	directory id*		
ModifyWorkspaceProperties	Grants permission to modify WorkSpace properties, including the running mode and the AutoStop period	Write	workspace id*		
ModifyWorkspaceState	Grants permission to modify the state of WorkSpaces	Write	workspace id*		
RebootWorkspaces	Grants permission to reboot WorkSpaces	Write	workspace id*		
RebuildWorkspaces	Grants permission to rebuild WorkSpaces	Write	workspace id*		
RegisterWorkspaceDirectory	Grants permission to register directories for use with Amazon WorkSpaces	Write	directory id*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectAccountLinkInvitation	Grants permission to reject invitations from other AWS 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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateConsent [permission only]	Grants permission to update the consent agreement to BYOL minimum requirements	Write			
UpdateRootClientCertificate [permission only]	Grants permission to update a root client certificate	Write	certificateid*		

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
certificateid	arn:${Partition}:workspaces:${Region}:${Account}:workspacecertificate/${CertificateId}	
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 AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString
workspaces:userId	Filters access by the ID of the Workspaces user	String

Actions, resources, and condition keys for Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager (service prefix: `wam`) 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 Application Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthenticatePackager [permission only]	Allows the Amazon WAM packaging instance to access your application package catalog.	Write			

Resource types defined by Amazon WorkSpaces Application Manager

Amazon WorkSpaces Application Manager does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon WorkSpaces Application Manager, specify `"Resource": "*"` in your policy.

Condition keys for Amazon WorkSpaces Application Manager

WAM has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS WorkSpaces Managed Instances

AWS WorkSpaces Managed Instances (service prefix: `workspaces-instances`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

Actions defined by AWS WorkSpaces Managed Instances

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action

with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Volume	Grants permission to associate a workspace managed volume to a workspace managed instance in your account	Write	WorkspaceInstanceId*		ec2:AttachVolume ec2:DescribeVolumes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVolume	Grants permission to create a workspace managed volume in your account	Write			ec2:CreateVolume
CreateWorkspaceInstance	Grants permission to create a workspace managed instance in your account	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeInstances ec2:RunInstances
DeleteVolume	Grants permission to delete a workspace managed volume in your account	Write	VolumeId*		ec2:DeleteVolume ec2:DescribeVolumes
DeleteWorkspaceInstance	Grants permission to delete a workspace managed instance in your account	Write	WorkspaceInstanceId*		ec2:TerminateInstances
DisassociateVolume	Grants permission to disassociate a workspace managed volume from a workspace managed instance in your account	Write	WorkspaceInstanceId*		ec2:DescribeVolumes ec2:DetachVolume
GetWorkspaceInstance	Grants permission to get details for a specific workspace managed instance in your account	Read	WorkspaceInstanceId*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstanceTypes	Grants permission to list all supported instance types	List			
ListRegions	Grants permission to list all supported AWS regions	List			
ListTagsForResource	Grants permission to list user tags for resources in your account	List	WorkspaceInstanceId*		
ListWorkspaceInstances	Grants permission to list workspace managed instances in your account	List			
TagResource	Grants permission to add user tags to resources in your account	Tagging	WorkspaceInstanceId*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove user tags from resources in your account	Tagging	WorkspaceInstanceId*		
				aws:TagKeys	

Resource types defined by AWS WorkSpaces Managed Instances

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
WorkspaceInstanceId	`arn:${Partition}:workspaces-instances:${Region}:${Account}:workspaceinstance/${WorkspaceInstanceId}`	aws:ResourceTag/${TagKey}
VolumeId	`arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS WorkSpaces Managed Instances

AWS WorkSpaces Managed Instances defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser (service prefix: `workspaces-web`) 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 Secure Browser

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate BrowserSettings	Grants permission to associate browser settings to web portals	Write	browserSettings*		
			portal*		
Associate DataProtectionSettings	Grants permission to associate data protection settings with web portals	Write	dataProtectionSettings*		
			portal*		
Associate IpAccessSettings	Grants permission to associate ip access settings with web portals	Write	ipAccessSettings*		
			portal*		
Associate NetworkSettings	Grants permission to associate network settings to web portals	Write	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkI

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					nterfaceP ermission ec2:Modif yNetworkI nterfaceA ttribute
			portal*		
Associate SessionLo gger	Grants permission to associate session logger with web portals	Write	portal*		
			sessionLo gger*		
Associate TrustStore	Grants permission to associate trust stores with web portals	Write	portal*		
			trustStor e*		
Associate UserAcces sLoggingS ettings	Grants permission to associate user access logging settings with web portals	Write	portal*		kinesis:P utRecord kinesis:P utRecords
			userAcces sLoggingS ettings*		
Associate UserSettings	Grants permission to associate user settings with web portals	Write	portal*		
			userSetti ngs*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBrowserSettings	Grants permission to create browser settings	Write		aws:TagKeys aws:RequestTag/${TagKey}	kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey workspaces-web:TagResource
CreateDataProtectionSettings	Grants permission to create data protection settings	Write		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateIdentityProvider	Grants permission to create identity providers	Write	identityProvider* portal*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIpAccessSettings	Grants permission to create ip access settings	Write		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateNetworkSettings	Grants permission to create network settings	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole workspaces-web:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePortal	Grants permission to create web portals	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey workspaces-web:TagResource
CreateSessionLogger	Grants permission to create session logger	Write		aws:TagKeys aws:RequestTag/${TagKey}	s3:PutObject workspaces-web:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrustStore	Grants permission to create trust stores	Write		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateUserAccessLoggingSettings	Grants permission to create user access logging settings	Write		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
CreateUserSettings	Grants permission to create user settings	Write		aws:TagKeys aws:RequestTag/${TagKey}	workspaces-web:TagResource
DeleteBrowserSettings	Grants permission to delete browser settings	Write	browserSettings*		
DeleteDataProtectionSettings	Grants permission to delete data protection settings	Write	dataProtectionSettings*		
DeleteIdentityProvider	Grants permission to delete identity providers	Write	identityProvider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			portal*		
DeleteIpAccessSettings	Grants permission to delete ip access settings	Write	ipAccessSettings*		
DeleteNetworkSettings	Grants permission to delete network settings	Write	networkSettings*		
DeletePortal	Grants permission to delete web portals	Write	portal*		
DeleteSessionLogger	Grants permission to delete session logger	Write	sessionLogger*		
DeleteTrustStore	Grants permission to delete trust stores	Write	trustStore*		
DeleteUserAccessLoggingSettings	Grants permission to delete user access logging settings	Write	userAccessLoggingSettings*		
DeleteUserSettings	Grants permission to delete user settings	Write	userSettings*		
DisassociateBrowserSettings	Grants permission to disassociate browser settings from web portals	Write	portal*		
DisassociateDataProtectionSettings	Grants permission to disassociate data protection logging from web portals	Write	portal*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIpAccessSettings	Grants permission to disassociate ip access logging from web portals	Write	portal*		
DisassociateNetworkSettings	Grants permission to disassociate network settings from web portals	Write	portal*		
DisassociateSessionLogger	Grants permission to disassociate session logger from web portals	Write	portal*		
DisassociateTrustStore	Grants permission to disassociate trust stores from web portals	Write	portal*		
DisassociateUserAccessLoggingSettings	Grants permission to disassociate user access logging settings from web portals	Write	portal*		
DisassociateUserSettings	Grants permission to disassociate user settings from web portals	Write	portal*		
ExpireSession	Grants permission to expire a session from a specific portal	Write	portal*		
GetBrowserSettings	Grants permission to get details on browser settings	Read	browserSettings*		
GetDataProtectionSettings	Grants permission to get details on data protection settings	Read	dataProtectionSettings*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdentityProvider	Grants permission to get details on identity providers	Read	identityProvider*		
GetIpAccessSettings	Grants permission to get details on ip access settings	Read	ipAccessSettings*		
GetNetworkSettings	Grants permission to get details on network settings	Read	networkSettings*		
GetPortal	Grants permission to get details on web portals	Read	portal*		
GetPortalServiceProviderMetadata	Grants permission to get service provider metadata information for web portals	Read	portal*		
GetSession	Grants permission to get information about a particular session for a portal	Read	portal*		
GetSessionLogger	Grants permission to get details on session logger	Read	sessionLogger*		
GetTrustStore	Grants permission to get details on trust stores	Read	trustStore*		
GetTrustStoreCertificate	Grants permission to get certificates from trust stores	Read	trustStore*		
GetUserAccessLoggingSettings	Grants permission to get details on user access logging settings	Read	userAccessLoggingSettings*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserSettings	Grants permission to get details on user settings	Read	userSettings*		
ListBrowserSettings	Grants permission to list browser settings	Read			
ListDataProtectionSettings	Grants permission to list data protection settings	Read			
ListIdentityProviders	Grants permission to list identity providers	Read	identityProvider*		
ListIpAccessSettings	Grants permission to list ip access settings	Read			
ListNetworkSettings	Grants permission to list network settings	Read			
ListPortals	Grants permission to list web portals	Read			
ListSessionLoggers	Grants permission to list session loggers	Read			
ListSessions	Grants permission to list sessions for a Portal using optional filters	Read	portal*		
ListTagsForResource	Grants permission to list tags for a resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrustStoreCertificates	Grants permission to list certificates in a trust store	Read			
ListTrustStores	Grants permission to list trust stores	Read			
ListUserAccessLoggingSettings	Grants permission to list user access logging settings	Read			
ListUserSettings	Grants permission to list user settings	Read			
TagResource	Grants permission to add one or more tags to a resource	Tagging	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		
			networkSettings		
			portal		
			sessionLogger		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	browserSettings		
			dataProtectionSettings		
			identityProvider		
			ipAccessSettings		
			networkSettings		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			portal		
			sessionLogger		
			trustStore		
			userAccessLoggingSettings		
			userSettings		
				aws:TagKeys	
UpdateBrowserSettings	Grants permission to update browser settings	Write	browserSettings*		
UpdateDataProtectionSettings	Grants permission to update data protection settings	Write	dataProtectionSettings*		
UpdateIdentityProvider	Grants permission to update identity provider	Write	identityProvider*		
			portal*		
UpdateIpAccessSettings	Grants permission to update ip access settings	Write	ipAccessSettings*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNetworkSettings	Grants permission to update network settings	Write	networkSettings*		ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateTags ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:ModifyNetworkInterfaceAttribute
UpdatePortal	Grants permission to update web portals	Write	portal*		
UpdateSessionLogger	Grants permission to update session logger	Write	sessionLogger*		
UpdateTrustStore	Grants permission to update trust stores	Write	trustStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUserAccessLoggingSettings	Grants permission to update user access logging settings	Write	userAccessLoggingSettings*		kinesis:PutRecord kinesis:PutRecords
UpdateUserSettings	Grants permission to update user settings	Write	userSettings*		

Resource types defined by Amazon WorkSpaces Secure Browser

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
browserSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:browserSettings/${BrowserSettingsId}`	aws:ResourceTag/${TagKey}
identityProvider	`arn:${Partition}:workspaces-web:${Region}:${Account}:identityProvider/${PortalId}/${IdentityProviderId}`	aws:ResourceTag/${TagKey}
networkSettings	`arn:${Partition}:workspaces-web:${Region}:${Account}:networkSettings/${NetworkSettingsId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
portal	arn:${Partition}:workspaces-web:${Region}:${Account}:portal/${PortalId}	aws:ResourceTag/${TagKey}
trustStore	arn:${Partition}:workspaces-web:${Region}:${Account}:trustStore/${TrustStoreId}	aws:ResourceTag/${TagKey}
userSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userSettings/${UserSettingsId}	aws:ResourceTag/${TagKey}
userAccessLoggingSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:userAccessLoggingSettings/${UserAccessLoggingSettingsId}	aws:ResourceTag/${TagKey}
ipAccessSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:ipAccessSettings/${IpAccessSettingsId}	aws:ResourceTag/${TagKey}
dataProtectionSettings	arn:${Partition}:workspaces-web:${Region}:${Account}:dataProtectionSettings/${DataProtectionSettingsId}	aws:ResourceTag/${TagKey}
sessionLogger	arn:${Partition}:workspaces-web:${Region}:${Account}:sessionLogger/${SessionLoggerId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client (service prefix: `thinclient`) 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 Thin Client
- Resource types defined by Amazon WorkSpaces Thin Client
- Condition keys for Amazon WorkSpaces Thin Client

Actions defined by Amazon WorkSpaces Thin Client

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEnvironment	Grants permission to create environments	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	appstream:DescribeStacks iam:CreateServiceLinkedRole workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories
DeleteDevice	Grants permission to delete devices	Write	device*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEnvironment	Grants permission to delete environments	Write	environment*		
				aws:ResourceTag/${TagKey}	
DeregisterDevice	Grants permission to deregister devices	Write	device*		
				aws:ResourceTag/${TagKey}	
GetDevice	Grants permission to get devices	Read	device*		
				aws:ResourceTag/${TagKey}	
GetDeviceDetails [permission only]	Grants permission to get details of devices	Read	device*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Grants permission to get details of environments	Read	environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetSoftwareSet	Grants permission to get details of software sets	Read	softwareset*		
				aws:ResourceTag/${TagKey}	
ListDeviceSessions [permission only]	Grants permission to list device sessions	List	device*		
				aws:ResourceTag/${TagKey}	
ListDevices	Grants permission to list devices	List			
ListEnvironments	Grants permission to list environments	List			
ListSoftwareSets	Grants permission to list software sets	List			
ListTagsForResource	Grants permission to list tags for a resource	List	device		
			environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			softwareset		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to add one or more tags to a resource	Tagging	device		
			environment		
			softwareset		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	device		
			environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			softwareset		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateDevice	Grants permission to update devices	Write	device*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update environments	Write	environment*		appstream:DescribeStacks workspaces-web:GetPortal workspaces-web:GetUserSettings workspaces:DescribeWorkspaceDirectories
				aws:ResourceTag/${TagKey}	
UpdateSoftwareSet	Grants permission to update software set	Write	softwareset*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon WorkSpaces Thin Client

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:${Partition}:thinclient:${Region}:${Account}:environment/${EnvironmentId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:thinclient:${Region}:${Account}:device/${DeviceId}`	aws:ResourceTag/${TagKey}
softwareset	`arn:${Partition}:thinclient:${Region}:${Account}:softwareset/${SoftwareSetId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS X-Ray

AWS X-Ray (service prefix: `xray`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS X-Ray
- Resource types defined by AWS X-Ray
- Condition keys for AWS X-Ray

Actions defined by AWS X-Ray

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetTraceSummaryById [permission only]	Grants permission to retrieve metadata for a list of traces specified by ID	Read			
BatchGetTraces	Grants permission to retrieve a list of traces specified by ID. Each trace is a collection of segment documents that originates from a single request. Use GetTraceSummaries to get a list of trace IDs	List			
CancelTraceRetrieval	Grants permission to cancel an ongoing trace retrieval job initiated by StartTraceRetrieval using the provided RetrievalToken. A successful cancellation will return an HTTP 200 response	Read			
CreateGroup	Grants permission to create a group resource with a name and a filter expression	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSamplingRule	Grants permission to create a rule to control sampling behavior for instrumented applications	Write	sampling-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	Grants permission to delete a group resource	Write	group*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Grants permission to delete resource policies	Write		xray:ResourcePolicyName	
DeleteSamplingRule	Grants permission to delete a sampling rule	Write	sampling-rule*		
				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		xray:ResourcePolicyName	
PutSpans	Grants permission to upload OpenTelemetry spans to AWS X-Ray	Write		logs:LogGeneratingResourceArns	
PutSpansForIndexing [permission only]	Grants permission to upload spans to AWS X-Ray to be indexed	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTelemetryRecords	Grants permission to send AWS X-Ray daemon telemetry to the service	Write			
PutTraceSegments	Grants permission to upload segment documents to AWS X-Ray. The X-Ray SDK generates segment documents and sends them to the X-Ray daemon, which uploads them in batches	Write		logs:LogGeneratingResourceArns	
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			sampling-rule		
				aws:TagKeys	
UpdateGroup	Grants permission to update a group resource	Write	group*		
				aws:ResourceTag/${TagKey}	
UpdateIndexingRule	Grants permission to modify an indexing rule's configuration	Write			
UpdateSamplingRule	Grants permission to modify a sampling rule's configuration	Write	sampling-rule*		
				aws:ResourceTag/${TagKey}	
UpdateTraceSegmentDestination	Grants permission to modify the destination of data sent to PutTraceSegments and OpenTelemetry API	Write		xray:TraceSegmentDestination	

Resource types defined by AWS X-Ray

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	aws:ResourceTag/${TagKey}
sampling-rule	`arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}`	aws:ResourceTag/${TagKey}

Condition keys for AWS X-Ray

AWS X-Ray defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Condition keys	Description	Type
logs:LogGenerating ResourceArns	Filters access by LogGeneratingResourceArn in the request	ArrayOfARN
xray:ResourcePolicyName	Filters access by PolicyName in the request	String
xray:TraceSegmentDestination	Filters access by TraceSegmentDestination type in the request	String

Related resources

For related information found in the *IAM User Guide*, see the following resources:

- Tutorial: Create and attach your first customer managed policy
- AWS services that work with IAM
- Policy evaluation logic

Simplified AWS service information for programmatic access

AWS provides service reference information in JSON format to streamline the automation of policy management workflows. With the service reference information, you can access available operations, actions, resources, and condition keys across AWS services from machine-readable files. Service reference information includes metadata beyond authorization details, including IAM action last accessed information and IAM Access Analyzer policy generation data.

Security administrators can establish guardrails and developers can ensure appropriate access to applications by identifying the available actions, resources, and condition keys for each AWS service. AWS provides service reference information for AWS services to allow you to incorporate the metadata into your policy management workflows.

- For an inventory of actions, resources, and condition keys for use in IAM policies, see the Service Authorization Reference page for the AWS service. Actions, resources, and condition keys for services that share a service prefix may be split across multiple pages in the Service Authorization Reference.
- For a list of AWS services and actions for which IAM action last accessed information is displayed, see IAM action last accessed information services and actions in the IAM User Guide.
- For a list of AWS services and actions for which IAM Access Analyzer generates policies with action-level information, see IAM Access Analyzer policy generation services in the IAM User Guide.

The content presented in the Service Authorization Reference may be presented differently or contain different metadata. For more information, see Additional field definitions.

The service reference information also offers metadata on operations, including information on authorized actions and the method names in SDKs.

Additional context of the value of condition keys may be available to assist in scoping permissions. For example, the value of `iam:PassedToService` may appear when the action `iam:PassRole` is authorized by an operation.

This operation to action mapping is not supported for all services. Services that don't yet support this mapping will omit the AuthorizedAction property. Additionally, authorized action information

for operations does not include permissions that might be required for operations called on your behalf with Forward Access Sessions.

> **Note**
>
> Changes to the service reference information may take up to 24 hours to be reflected in the list of metadata for the service.

Accessing AWS service reference information

1. Navigate to the service reference information to access the list of AWS services for which reference information is available.

   There are two main entry points:

   http://servicereference.us-east-1.amazonaws.com/ displays a list of AWS services for which reference information is available.

   The following example shows a partial list of services and URLs for their respective reference information:

   ```
   [
       {
           "service": "s3",
           "url": "https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json"
       },
       {
           "service": "dynamodb",
           "url": "https://servicereference.us-east-1.amazonaws.com/v1/dynamodb/
   dynamodb.json"
       },
       …
   ]
   ```

   https://servicereference.us-east-1.amazonaws.com/v1/mapping.json displays a mapping from SDK services to the location in the service reference that information can be found under.

   The following example shows a partial list of mappings:

   ```
   {
   ```

```
  "SDK" : {
    "Python" : {
      "Boto3" : {
        "accessanalyzer" : {
          "service" : "access-analyzer",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/access-
analyzer/access-analyzer.json"
        },
        "account" : {
          "service" : "account",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/account/
account.json"
        },
        "amp" : {
          "service" : "aps",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/aps/
aps.json"
        },
        ...
      }
    }
  }
}
```

2. Choose a service and navigate to the service information page in the `url` field for the service to view a list of actions, resources, and condition keys for the service.

   The following example shows a partial list of service reference information for Amazon S3:

```
{
    "Name": "s3",
    "Actions": [
        {
            "Name": "GetObject",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
```

```
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
            "Properties" : {
                    "IsList" : false,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "object"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : true,
```

```
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "bucket"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Operations": [
        {
            "Name" : "GetObject",
            "AuthorizedActions" : [
                {
                    "Name" : "GetObject",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObject",
                    "Service" : "s3-object-lambda"
                }, {
                    "Name" : "GetObjectLegalHold",
```

```
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectRetention",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectTagging",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectVersion",
                    "Service" : "s3"
                }
            ],
            "SDK" : [
                {
                    "Name" : "s3",
                    "Method" : "get_object",
                    "Package" : "Boto3"
                }
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.4"
}
```

3. Download the JSON file from the service URL to use in your policy authoring workflows.

Glossary

- Operation - An API that can be called, usually through an SDK
- Action - Permission that is authorized when performing an operation

Additional field definitions

Action properties provide additional metadata about service actions to help categorize them based on their permission scope. These properties are found under the `Annotations` field for each action. The metadata consists of four boolean values:

- `IsList` – Provides permissions to discover and list resources, including basic metadata, without accessing resource contents.

  Example – This property is `true` for the Amazon S3 `ListBucket` action, allowing users to view bucket listings without accessing the objects themselves.
- `IsPermissionManagement` – Provides permissions to modify IAM permissions or access credentials.

  Example – This property is `true` for most IAM and AWS Organizations actions, as well as Amazon S3 actions like `PutBucketPolicy` and `DeleteBucketPolicy`.
- `IsTaggingOnly` – Provides permissions only for modifying tags.

  Example – This property is `true` for IAM actions `TagRole` and `UntagRole`, while this property is `false` for `CreateRole` since it provides broader permissions beyond tagging.
- `IsWrite` – Provides permissions to modify resources, which may include tag modifications.

  Example – This property is `true` for Amazon S3 actions `CreateBucket`, `DeleteBucket`, and `PutObject` since they allow resource modification.

> **Note**
>
> These properties are not mutually exclusive. An action may have multiple properties set to `true`.
> It's also possible for all properties to be `false`, as seen with Amazon S3's `GetObject` action. This indicates the action only grants read permissions on an object.

These properties can be used to generate insights for services. The following example shows which permissions with the s3 prefix allow mutating resources:

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsWrite == true) | .Name'

"AssociateAccessGrantsIdentityCenter"
"BypassGovernanceRetention"
"CreateAccessGrant"
"CreateAccessGrantsInstance"
"CreateAccessGrantsLocation"
...
```

The following example shows which action condition keys with the lambda prefix you can use to limit access to permission management actions:

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/lambda/lambda.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsPermissionManagement == true) |
 {Name: .Name, ActionConditionKeys: (.ActionConditionKeys // [])}'

{
   "Name": "AddLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "AddPermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
{
    "Name": "DisableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "EnableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "RemoveLayerVersionPermission",
    "ActionConditionKeys": []
}
```

```
{
    "Name": "RemovePermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
```